Linking Entanglement Detection and State Tomography via Quantum 2-Designs

Bae, Joonwoo; Hiesmayr, Beatrix; McNulty, Daniel

Published in:
New Journal of Physics

DOI:
10.1088/1367-2630/aaf8cf

Publication date:
2019

Citation for published version (APA):
Bae, J., Hiesmayr, B., & McNulty, D. (2019). Linking Entanglement Detection and State Tomography via Quantum 2-Designs. *New Journal of Physics*, *21*, [013012]. https://doi.org/10.1088/1367-2630/aaf8cf

New Journal of Physics
The open access journal at the forefront of physics

Deutsche Physikalische Gesellschaft DPG IOP Institute of Physics

PAPER • OPEN ACCESS

Linking entanglement detection and state tomography via quantum 2-designs

To cite this article: Joonwoo Bae *et al* 2019 *New J. Phys.* **21** 013012

New Journal of Physics
The open access journal at the forefront of physics

Deutsche Physikalische Gesellschaft DPG
IOP Institute of Physics

Published in partnership with: Deutsche Physikalische Gesellschaft and the Institute of Physics

OPEN ACCESS

RECEIVED
15 August 2018

REVISED
9 November 2018

ACCEPTED FOR PUBLICATION
14 December 2018

PUBLISHED
18 January 2019

PAPER

Linking entanglement detection and state tomography via quantum 2-designs

Joonwoo Bae[1,2], **Beatrix C Hiesmayr**[3,6] and **Daniel McNulty**[4,5]

[1] School of Electrical Engineering, Korea Advanced Institute of Science and Technology (KAIST), 291 Daehak-ro, Yuseong-gu, Daejeon 34141, Republic of Korea
[2] Freiburg Institute for Advanced Studies (FRIAS), Albert-Ludwigs University of Freiburg, Albertstrasse 19, D-79104 Freiburg, Germany
[3] University of Vienna, Faculty of Physics, Boltzmanngasse 5, A-1090 Vienna, Austria
[4] Department of Mathematics, Aberystwyth University, Aberystwyth, United Kingdom
[5] Faculty of Informatics, Masaryk University, Brno, Czechia
[6] Author to whom any correspondence should be addressed.

E-mail: Beatrix.Hiesmayr@unvie.ac.at

Keywords: mutually unbiased bases, symmetric informationally complete POVM, entanglement detection

Abstract

We present an experimentally feasible and efficient method for detecting entangled states with measurements that extend naturally to a tomographically complete set. Our detection criterion for bipartite systems with equal dimensions is based on measurements from subsets of a quantum 2-design, e.g. mutually unbiased bases or symmetric informationally complete states, and has several advantages over standard entanglement witnesses. First, as more detectors in the measurement are applied, there is a higher chance of witnessing a larger set of entangled states, in such a way that the measurement setting converges to a complete setup for quantum state tomography. Secondly, our method is twice as effective as standard witnesses in the sense that both upper and lower bounds can be derived. Thirdly, the scheme can be readily applied to measurement-device-independent scenarios.

For quantum information applications it is often more interesting to learn if multipartite quantum states are entangled than to identify quantum states themselves [1, 2]. This is in fact what *direct detection of entanglement* executes, which utilizes an entanglement witness that works with individual measurements followed be post-processing of the outcomes [3], to provide an experimentally feasible approach for this task [4]. Entanglement detection under less assumptions, for instance, when detectors are not trusted [5–7] or dimensions are unknown [8], is of practical significance for cryptographic applications.

For the practical usefulness of entanglement detection, it is worth exploring the experimental resources. If *a priori* information about a quantum state is given, a set of entanglement witnesses may be constructed accordingly and exploited for entanglement detection. With no *a priori* information multiple entanglement witnesses may be required. One possible method is quantum state tomography which determines a d-dimensional quantum state with $O(d^2)$ measurements. Then, theoretical tools such as positive maps [9], e.g. partial transpose, or numerical tests involving semidefinite programming [10] can be applied. For entanglement witnesses, however, little is known about the minimal measurements for their realization. In fact, it may happen that repeating experiments for multiple witnesses may be less cost effective than state tomography [11], and quite possible that no useful information is obtained, neither for entanglement detection nor for quantum state identification. This raises questions on the usefulness of entanglement witnesses, in particular when *a priori* information about a particular state is not available.

A useful experimental setup for entanglement detection may distinguish the largest collection of entangled states with as few measurements as possible. It is noteworthy that a tomographically complete measurement can ultimately identify a quantum state so that theoretical tools may completely determine whether it is entangled or separable. From a practical point of view, it would be therefore highly desirable that measurements for entanglement detection are constructive, i.e. they can be extended to a tomographically complete set by augmenting more detectors.

In this work we establish a feasible and practical framework of entanglement detection by applying a subset of measurements taken from a quantum 2-design, namely mutually unbiased bases (MUBs) [12] and a

symmetric informationally complete (SIC) positive-operator-valued-measure (POVM) [13]. The connections between entanglement detection, MUBs, and quantum 2-designs have first been explored in [14, 15], and subsequent results were found in, e.g. [16–18]. Let us emphasize here that entanglement detection via MUBs can also detect bound entangled states, those mixed entangled states from which no entanglement can be distilled. Furthermore, measurement setups with MUBs are very experimentally friendly, indeed the MUB criterion [14] resulted in the first experimental demonstration of bipartite bound entanglement [19], predicted in 1998 [20]. Here we present a unifying approach to these connections with a three-fold advantage. First, by using incomplete sets of MUBs and subsets of a SIC-POVM, the entanglement detection scheme then extends naturally to an optimal reconstruction of the quantum state [21, 22]: once direct detection of entanglement fails, additional detectors are applied in the measurement scheme to distinguish a larger set of entangled states, and can be ultimately utilised to find its separability via state tomography. This demonstrates in a natural framework that larger sets of detectors are more useful for distinguishing entangled states. Next, our results have *twice* the efficiency of standard witnesses, in the sense that both a lower and upper bound for separable states exist, whereas entanglement witnesses have only the zero-valued lower bound. Finally, the scheme can be readily applied to a measurement-device-independent (MDI) scenario for which the assumptions on the detectors are relaxed. This can be achieved by converting the measurement into the preparation of a quantum 2-design.

Let us begin with a brief summary on the implementation of entanglement witnesses in practice. Entanglement witnesses correspond to observables that have non-negative expectation values for all separable states as well as negative values for some entangled states. They can be factorized into local observables in general, which are then decomposed by POVM elements [23]. A witness W can be written with POVMs denoted by $\{M_i^{(X)}\}$ for party $X = A, B$, where the measurement is complete, i.e. $\sum_i M_i^{(X)} = I_X$ where I_X denotes the identity operator on system X, as

$$W = \sum_i c_i M_i, \quad \text{where } M_i = M_i^{(A)} \otimes M_i^{(B)}, \tag{1}$$

with constants $\{c_i\}$. In implementation, a POVM can be realized by projective measurements with ancillary systems, see e.g. [24]. For a state ρ, the probabilities $\Pr[M_i|\rho] = \mathrm{tr}[\rho M_i]$ are estimated experimentally by the detectors $\{M_i\}$. Then, the expectation value of W for a state ρ is obtained by computing the linear combination, $\sum_i c_i \Pr[M_i|\rho]$, which equals $\mathrm{tr}[W\rho]$.

Although the factorization with local measurements in equation (1) is not necessary to realize entanglement witnesses, it provides a natural framework for converting standard entanglement witnesses to the MDI scenario that closes all loopholes arising from detectors. In such a scenario two parties Alice and Bob, who want to learn if an unknown quantum state ρ_{AB} is entangled, prepare a set of quantum states, after which a measurement is performed by untrusted parties. A standard witness in equation (1) can be used to construct an MDI entanglement witness as follows

$$W_{\mathrm{MDI}} = \sum_i c_i M_i^{(A)\top} \otimes M_i^{(B)\top}, \tag{2}$$

where the transpose $\top$ is performed in a chosen basis of $\mathcal{H}_Y$ for $Y = A, B$ [6]. The separable decomposition in equation (2) shows which quantum states the two parties must prepare, $\{\widetilde{M}_i^{(A)}\}$ and $\{\widetilde{M}_i^{(B)}\}$, where $\widetilde{M}_i^{(Y)} = M_i^{(Y)}/\mathrm{tr}[M_i^{(Y)}]$ correspond to the quantum states.

Let us reiterate that entanglement witnesses with local measurements in equation (1) are readily converted to their counterparts in an MDI scenario, where entangled states are detected with less assumptions. We also note that, to the best of our knowledge, there is no general and systematic way of finding the factorization with a minimal number of local measurements. The decomposition with a minimal number of POVM elements is essential, as mentioned, to take advantage of entanglement witnesses that can detect entangled states without state tomography.

We now introduce particular sets of POVMs called quantum 2-designs. A set of quantum states $\{|\psi_i\rangle\}_k$ in a d-dimensional Hilbert space, $|\psi_i\rangle \in \mathcal{H}_d$, or their corresponding rank-one projectors, is called a quantum 2-design if the average value of any second order polynomial over the set $\{|\psi_i\rangle\}_k$ is equal to the average $f(\psi)$ over all normalized states $|\psi\rangle$, for the Haar measure. This holds true if and only if the average of $|\psi_i\rangle\langle\psi_i|^{\otimes 2}$ over the entire 2-design is proportional to the symmetric projection onto $\mathcal{H}_d \otimes \mathcal{H}_d$. Examples of quantum 2-designs include a complete set of $(d+1)$ MUBs, and a SIC-POVM containing d^2 elements, which are defined as follows.

Let $\mathcal{B}_k = \{|b_i^k\rangle\}_{i=1}^d$ denote an orthonormal basis in the Hilbert space $\mathcal{H}_d$. A set of m bases $\{\mathcal{B}_k\}_{k=1}^m$ are mutually unbiased if

$$|\langle b_i^k|b_{i'}^{k'}\rangle|^2 = \frac{1}{d}(1 - \delta_{kk'}) + \delta_{ii'}\delta_{kk'}, \tag{3}$$

for $i, i' = 1,\ldots, d$, and $k, k' = 1,\ldots, m$. Let $S_d = \{|s_j\rangle\}_{j=1}^{d^2}$ denote a set of d^2 vectors in the same Hilbert space $\mathcal{H}_d$. The set S_d is a SIC-POVM if

$$|\langle s_j|s_{j'}\rangle|^2 = \frac{d\delta_{jj'}+1}{(d+1)}, \tag{4}$$

for all $j, j' = 1,\ldots, d^2$.

The existence of $(d+1)$ MUBs and d^2 SIC states in all dimensions have been long-standing open problems in quantum information theory [25]. For instance, complete sets of MUBs are known to exist in prime-power dimensions [21, 26–29] but have not been found in in any other composite dimension. For example, when $d = 6$, it is conjectured that only 3 MUBs exist [30, 31], but no proof exists. While it is conjectured that a SIC-POVM exists for any d, the largest dimension for which an exact solution has been found is $d = 323$ [32].

It is well known that a full set of $(d+1)$ MUBs and a SIC-POVM are tomographically complete: measurements from either set determine a quantum state uniquely. Furthermore, the sets are both optimal and simple for quantum state tomography, in that they minimize the error of the estimated statistics while at the same time having exceptionally simple state reconstruction formulas [21, 22]. Note that both MUBs and SIC-POVMs are experimentally feasible, and have been implemented for the purpose of state tomography. A recent demonstration has been given in [33].

We now consider subsets of $(d+1)$ MUBs and d^2 SIC vectors for detecting entangled states. We denote by $I^{(\mathrm{M})}_{m,d}$ and $I^{(\mathrm{S})}_{\widetilde{m},d}$ the collections of probabilities when the measurements are applied in MUBs and SICs, respectively,

$$I^{(\mathrm{M})}_{m,d}(\rho\colon \{\mathcal{B}_k\}_{k=1}^{m}) = \sum_{k=1}^{m}\sum_{i=1}^{d}\Pr(i,\, i|\mathcal{B}_k,\, \mathcal{B}_k), \tag{5}$$

$$I^{(\mathrm{S})}_{\widetilde{m},d}(\rho\colon S_{\widetilde{m}}) = \sum_{j=1}^{\widetilde{m}}\Pr(j,\, j|S_{\widetilde{m}},\, S_{\widetilde{m}}), \tag{6}$$

where $S_{\widetilde{m}}$ denotes a collection of $\widetilde{m}$ states out of d^2 SIC vectors, and $\Pr(\alpha,\, \beta|A,\, B)$ the probability of obtaining outcome $(\alpha,\, \beta)$ given a measurement in A and B. To be explicit, for state ρ, $\Pr(i,\, i|\mathcal{B}_k,\, \mathcal{B}_k) = \mathrm{tr}[|b_i^k\rangle\langle b_i^k|\otimes|b_i^k\rangle\langle b_i^k|\,\rho]$[7] and $\Pr(j,\, j|S_{\widetilde{m}},\, S_{\widetilde{m}}) = \mathrm{tr}[|s_j\rangle\langle s_j|\otimes|s_j\rangle\langle s_j|\,\rho]$. These probabilities can be obtained simply by preparing local measurements in MUBs or SICs. Note that we have $m \leqslant d+1$ and $\widetilde{m} \leqslant d^2$, where the equality corresponds to cases in which the measurement setting is tomographically complete.

Since the set of all separable states forms a convex set, the quantities $I^{(\mathrm{M})}_{m,d}$ and $I^{(\mathrm{S})}_{\widetilde{m},d}$ as defined in equations (5) and (6) have both nontrivial upper and lower bounds satisfied by all separable states. In what follows, the bounds for selections of m MUBs and $\widetilde{m}$ SIC vectors are explicitly presented. We minimize and maximize each of the bounds with respect to the set of MUBs and SIC vectors, e.g. minimizing (maximizing) the lower bound over all MUBs gives $L^{-(\mathrm{M})}_{m,d}$ ($L^{+(\mathrm{M})}_{m,d}$). The former (latter) gives a bound which is independent (dependent) of the choice of MUBs. Consequently, $L^{+(\mathrm{M})}_{m,d}$ detects a larger set of entangled states but only applies for a certain collection of MUBs.

When the measurements are taken from a set of MUBs, the minimal and maximal lower bounds, $L^{-(\mathrm{M})}_{m,d}$ and $L^{+(\mathrm{M})}_{m,d}$, respectively, are given by

$$L^{-(\mathrm{M})}_{m,d} = \min_{\{\mathcal{B}_k\}_{k=1}^{m}}\min_{\sigma_{\mathrm{sep}}} I^{(\mathrm{M})}_{m,d}(\sigma_{\mathrm{sep}}\colon \{\mathcal{B}_k\}_{k=1}^{m}), \tag{7}$$

$$L^{+(\mathrm{M})}_{m,d} = \max_{\{\mathcal{B}_k\}_{k=1}^{m}}\min_{\sigma_{\mathrm{sep}}} I^{(\mathrm{M})}_{m,d}(\sigma_{\mathrm{sep}}\colon \{\mathcal{B}_k\}_{k=1}^{m}), \tag{8}$$

where the optimisation is taken over all separable states σ_{sep} and all possible collections of m MUBs, $\{\mathcal{B}_k\}_{k=1}^{m}$, that exist in dimension d. It is clear that $L^{+(\mathrm{M})}_{m,d} \geqslant L^{-(\mathrm{M})}_{m,d}$, and the gap between the bounds is due to different sets of m MUBs having different overlaps with the set of separable states.

Unfortunately, we do not find a systematic and general method of obtaining these bounds but had to consider all possible sets of m MUBs, minimizing $I^{(\mathrm{M})}_{m,d}$ over all separable states. In table 1, lower bounds are shown for $d = 2,\, 3,\, 4$, which are obtained analytically. It turns out that $L^{-(\mathrm{M})}_{m,d} = L^{+(\mathrm{M})}_{m,d}$ for $d = 2, 3$, but for $d = 4$ we found $L^{-(\mathrm{M})}_{m,4} \geqslant L^{+(\mathrm{M})}_{m,4}$. The difference here is due to the existence of an infinite family of 3 MUBs in $d = 4$, resulting in unitarily inequivalent triples. The triple which gives $L^{-(\mathrm{M})}_{m,4} = 1/4$ is the only extendible set of 3 MUBs, in the sense that no other triple extends to a complete set of 5 MUBs. For $d = 2,\, 3$, all subsets of m MUBs are equivalent and extendible.

In [14], it has been shown that the upper bound does not depend on selections of MUBs, and is given by

$$U^{(\mathrm{M})}_{m,d} = \max_{\sigma_{\mathrm{sep}}} I^{(\mathrm{M})}_{m,d}(\sigma_{\mathrm{sep}} : \{\mathcal{B}_k\}_{k=1}^{m}) = 1 + \frac{m-1}{d}, \tag{9}$$

for any m MUBs $\{\mathcal{B}_k\}_{k=1}^{m}$. Note that in the case of a quantum 2-design with $m = d+1$, the upper bound satisfies $U^{(\mathrm{M})}_{d+1,d} = 2$, which is independent of the dimension d. Notice also that by removing a single basis from

[7] Note that Alice and Bob may consider an unphysical relabelling of their basis vectors in order to optimize the correlation function. In particular, for the isotropic state a complex conjugation in one subsystem gives the optimum.

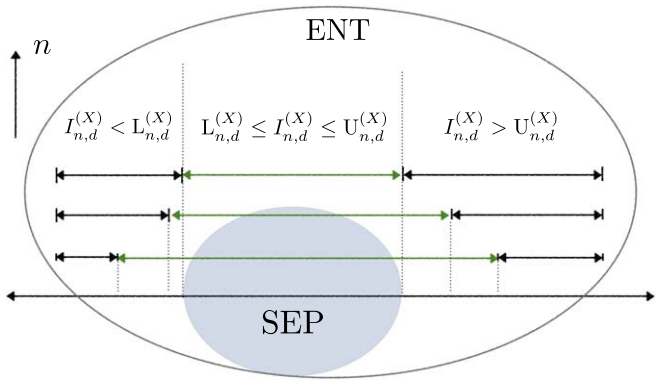

Figure 1. Our strategy for detecting entangled states via MUBs and SICs is illustrated, where $X = \mathrm{M},\ \mathrm{S}$ and $n = m,\ \widetilde{m}$, see inequalities in equations (10) and (13) satisfied by all separable states. Violation of the bounds implies detection of entangled states. Once the measurement outcomes are collected, they are exploited *twice* to find if the upper or lower bound is violated, in which case entangled states are detected.

Table 1. Lower and upper bounds on MUBs, $L_{m,d}^{\pm(\mathrm{M})}$ and $U_{m,d}^{(\mathrm{M})}$, see equations (7)–(9), are summarized for m MUBs in $\mathcal{H} = \mathbb{C}^d$, for $d = 2,\ 3,\ 4$. For $d = 2, 3$, inequivalent sets of m MUBs do not exist, hence we have $L_{m,d}^{+(\mathrm{M})} = L_{m,d}^{-(\mathrm{M})}$. This is no longer true for $d = 4$, as seen when $m = 3$.

	Lower bounds				Upper bounds		
			$d = 4$				
m	$d = 2$ $L_{m,2}^{(\mathrm{M})}$	$d = 3$ $L_{m,3}^{(\mathrm{M})}$	$L_{m,4}^{-(\mathrm{M})}$	$L_{m,4}^{+(\mathrm{M})}$	$d = 2$ $U_{m,2}^{(\mathrm{M})}$	$d = 3$ $U_{m,3}^{(\mathrm{M})}$	$d = 4$ $U_{m,4}^{(\mathrm{M})}$
2	1/2	0.211	0	0	3/2	4/3	5/4
3	1	1/2	1/4	1/2	2	5/3	6/4
4		1	1/2	1/2		2	7/4
5			1	1			2

$I_{m,d}^{(\mathrm{M})}$ the upper bound decreased uniformly by $1/d$, i.e.

$$U_{m+1,d}^{(\mathrm{M})} - U_{m,d}^{(\mathrm{M})} = d^{-1}$$

for all m MUBs.

In our first main result, using table 1 and equation (9), we can construct the inequalities with optimization over m MUBs in equation (5) as

$$L_{m,d}^{-(\mathrm{M})} \leqslant I_{m,d}^{(\mathrm{M})}(\sigma_{\mathrm{sep}}) \leqslant U_{m,d}^{(\mathrm{M})}, \tag{10}$$

that are satisfied by all separable states in $\mathcal{H}_d \otimes \mathcal{H}_d$. A quantum state must be entangled if it violates one of the inequalities above, see also figure 1. It is also worth mentioning that these inequalities detect bound entangled states when $m = d + 1$, as shown in [19].

In a similar way, lower and upper bounds for SICs are denoted as follows, with $g = \pm$, and $\mathrm{opt}^{+} = \max$ and $\mathrm{opt}^{-} = \min$,

$$L_{\widetilde{m},d}^{g\,(\mathrm{S})} = \mathrm{opt}_{S_{\widetilde{m}} \subseteq S_{d^2}}^{g} \min_{\sigma_{\mathrm{sep}}} I_{\widetilde{m},d}^{(\mathrm{S})}(\sigma_{\mathrm{sep}}\colon S_{\widetilde{m}}) \text{ and} \tag{11}$$

$$U_{\widetilde{m},d}^{g\,(\mathrm{S})} = \mathrm{opt}_{S_{\widetilde{m}} \subseteq S_{d^2}}^{g} \max_{\sigma_{\mathrm{sep}}} I_{\widetilde{m},d}^{(\mathrm{S})}(\sigma_{\mathrm{sep}}\colon S_{\widetilde{m}}), \tag{12}$$

where $S_{\widetilde{m}}$ is a set of $\widetilde{m}$ SIC vectors. Then, the full set of SIC vectors is denoted by S_d^2. Again, we do not find a systematic and general method of computing upper and lower bounds. However, having explored all possible subsets of SIC vectors in $d = 2, 3$, for a given SIC-POVM, we present these bounds in table 2. Suboptimal bounds for $d = 4$ are also presented in the appendix. We observe that $U_{\widetilde{m},d}^{+(\mathrm{S})} \geqslant U_{\widetilde{m},d}^{-(\mathrm{S})}$, i.e. differences in the subsets of SIC vectors give rise to the gap between these upper bounds. Therefore, the inequalities which are satisfied by all separable states are constructed in our second main result as

$$L_{\widetilde{m},d}^{-(\mathrm{S})} \leqslant I_{\widetilde{m},d}^{(\mathrm{S})}(\sigma_{\mathrm{sep}}) \leqslant U_{\widetilde{m},d}^{+(\mathrm{S})}, \tag{13}$$

Table 2. The lower and upper bounds via SICs, $L^{\pm(\mathrm{S})}_{\widetilde{m},d}$ and $U^{\pm(\mathrm{S})}_{\widetilde{m},d}$, are shown for $d = 2, 3$. We use the SIC-POVM defined in equations (B.28) for $d = 2$ and the Hesse SIC defined in equations (B.32) for $d = 3$. Note that $L^{+(\mathrm{S})}_{\widetilde{m},2} = L^{-(\mathrm{S})}_{\widetilde{m},2}$ and $U^{+(\mathrm{S})}_{\widetilde{m},2} = U^{-(\mathrm{S})}_{\widetilde{m},2}$. In contrast to MUBs, we find that $\mathrm{U}^{+(\mathrm{S})}_{\widetilde{m},d} \geqslant \mathrm{U}^{-(\mathrm{S})}_{\widetilde{m},d}$.

	Lower bounds			Upper bounds		
	$d = 2$	$d = 3$		$d = 2$	$d = 3$	
$\widetilde{m}$	$L^{(\mathrm{S})}_{\widetilde{m},2}$	$L^{-(\mathrm{S})}_{\widetilde{m},3}$	$L^{+(\mathrm{S})}_{\widetilde{m},3}$	$U^{(\mathrm{S})}_{\widetilde{m},2}$	$U^{+(\mathrm{S})}_{\widetilde{m},3}$	$U^{-(\mathrm{S})}_{\widetilde{m},3}$
3	0	0	0	1.244	1.254	9/8
4	4/15	0	0	4/3	1.400	1.25
5	2/3	0	0	4/3	1.463	1.400
6		0	0.112		3/2	1.482
7		3/20	3/20		3/2	3/2
8		3/8	3/8		3/2	3/2
9		3/4	3/4		3/2	3/2

where $L^{-(\mathrm{S})}_{\widetilde{m},d}$ and $U^{+(\mathrm{S})}_{\widetilde{m},d}$ are found in table 2. Even tighter inequalities with $L^{+(\mathrm{S})}_{\widetilde{m},d}$ and $U^{-(\mathrm{S})}_{\widetilde{m},d}$ can be derived by specifying the corresponding subset of $\widetilde{m}$ SIC vectors. We note that for large $\widetilde{m}$ the upper bounds become independent of the choice of SIC vectors, e.g. $U^{+(\mathrm{S})}_{\widetilde{m},3} = U^{-(\mathrm{S})}_{\widetilde{m},3} = 3/2$ for $\widetilde{m} = 7, 8, 9$.

While these inequalities have been obtained by extensively considering all sets of MUBs and SIC vectors, analytic expressions for the upper and lower bounds can be derived for a quantum 2-design

$$1 \leqslant I^{(\mathrm{M})}_{d+1,d}(\sigma_{\mathrm{sep}}) \leqslant 2, \quad \frac{d}{d+1} \leqslant I^{(\mathrm{S})}_{d^2,d}(\sigma_{\mathrm{sep}}) \leqslant \frac{2d}{d+1}, \tag{14}$$

as shown in the appendix. The upper bounds to $I^{(\mathrm{M})}_{d+1,d}$ and $I^{(\mathrm{S})}_{d^2,d}$ are proven in [14] and [17], respectively. Lower bounds are shown in [15] and later in [18]. As mentioned earlier, when the full measurement set of a quantum 2-design is used, it is more efficient to exploit the measurements for state tomography, and use theoretical tools to solve the separability problem that is known to be *NP*-hard.

To illustrate the effectiveness of the inequalities in equations (10) and (13), consider the isotropic and Werner states,

$$\text{Werner state:} \quad \rho_{\mathrm{W}}(p) = p\,\widetilde{\Pi}_{\mathrm{sym}} + (1-p)\,\widetilde{\Pi}_{\mathrm{asym}} \tag{15}$$

$$\text{isotropic state:} \quad \rho_{\mathrm{iso}}(q) = q|\Phi^+\rangle\langle\Phi^+| + (1-q)\mathbb{1}_d \otimes \mathbb{1}_d, \tag{16}$$

where $\widetilde{\Pi}_{\mathrm{sym}}$ and $\widetilde{\Pi}_{\mathrm{asym}}$ denote the normalized projections onto the symmetric and anti-symmetric subspaces, respectively, and $\mathbb{1}_d = \mathbb{1}/d$, the normalized identity operator in dimension d. We note that for a bipartite Hilbert space $\mathbb{C}^d \otimes \mathbb{C}^d$, the symmetric subspace is the subspace of all vectors in $\mathbb{C}^d \otimes \mathbb{C}^d$ which are symmetric under the interchange of their subsystems, while the anti-symmetric subspace is the subspace of all vectors that are negated by a permutation of their subsystems. It is known that ρ_{W} is entangled iff $p < 1/2$ and ρ_{iso} iff $q > (d+1)^{-1}$. In figure 2, the capability of entanglement detection with $I^{(\mathrm{M})}_{m,3}$ is shown for $m = 2, 3, 4$. The capability of entanglement detection via SICs is given in the appendix.

Due to the linearity of equations (5) and (6), with respect to the state ρ, one may expect that the inequalities in equation (14) are closely connected to standard entanglement witnesses. Here we point out the equivalence between the lower bounds in equation (14) and the partial transpose criterion, by considering the so-called structural physical approximation [1]. For recent reviews on this see [2], as well as the appendix for further details. The Choi–Jamiolkowski operator for the transpose map corresponds to an entanglement witness, denoted by W, i.e. $\mathrm{tr}[\sigma_{\mathrm{sep}} W] \geqslant 0$, and $\mathrm{tr}[\rho W] < 0$ for some entangled states ρ which include the entangled Werner states in equation (15). By applying the structural physical approximation to the transpose map, the resulting Choi–Jamiolkowski operator denoted by $\widetilde{W}$ is given by $\widetilde{W} = \widetilde{\Pi}_{\mathrm{sym}}$. The condition $\mathrm{tr}[\sigma_{\mathrm{sep}} W] \geqslant 0$ then translates to $\mathrm{tr}[\sigma_{\mathrm{sep}} \widetilde{W}] \geqslant [d(d+1)]^{-1}$, see [15], which is equivalent to the lower bounds in equation (14).

Finally, we can see that $I^{(\mathrm{M})}_{m,d}(\rho) = \mathrm{tr}[W^{(\mathrm{M})}_{m,d}\rho]$ and $I^{(\mathrm{S})}_{\widetilde{m},d}(\rho) = \mathrm{tr}[W^{(\mathrm{S})}_{\widetilde{m},d}\rho]$ are readily converted for entanglement detection in a MDI scenario where,

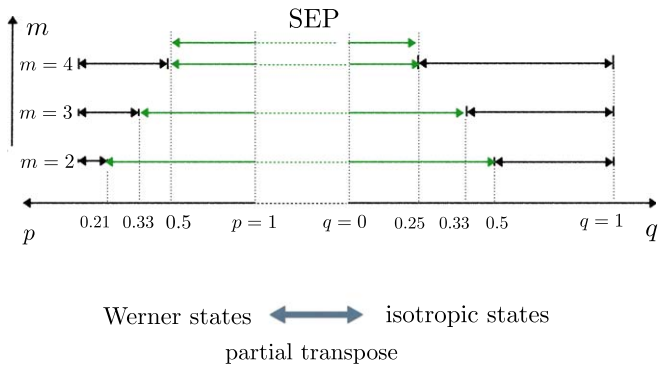

Figure 2. The inequalities $I^{(\mathrm{M})}_{2,3}$, $I^{(\mathrm{M})}_{3,3}$, and $I^{(\mathrm{M})}_{4,3}$ are applied to detect entangled states. Once $I_{m,d}(\mathrm{M})$ for unknown quantum states is obtained, it can be utilized twice for entanglement detection with both upper and lower bounds. E.g. the upper bounds are violated by entangled isotropic states and the lower bounds by entangled Werner states.

$$W^{(\mathrm{M})}_{m,d}(\{\mathcal{B}_k\}_{k=1}^{m}) = \sum_{k=1}^{m}\sum_{i=1}^{d} |b_i^k\rangle\langle b_i^k| \otimes |b_i^k\rangle\langle b_i^k|,$$

$$W^{(\mathrm{S})}_{\widetilde{m},d}(S_{\widetilde{m}}) = \sum_{j=1}^{\widetilde{m}} |s_j\rangle\langle s_j| \otimes |s_j\rangle\langle s_j|.$$

As described in equation (2), both $I^{(\mathrm{M})}_{m,d}$ and $I^{(\mathrm{S})}_{\widetilde{m},d}$ can be obtained in an MDI manner with $W^{(\mathrm{M})\top}_{m,d}(\{\mathcal{B}_k\}_{k=1}^{m})$ and $W^{(\mathrm{S})\top}_{\widetilde{m},d}(S_{\widetilde{m}})$, respectively, by preparing the set of quantum states $\{\mathcal{B}_k\}_{k=1}^{m}$ and $S_{\widetilde{m}}$ instead of measurements in these bases. Note also that this provides both upper and lower MDI bounds as opposed to standard MDI entanglement witnesses.

To conclude, let us recall the problem addressed at the outset. How do we learn efficiently if an unknown quantum state is entangled, with a measurement that is tomographically incomplete? In this paper we propose a measurement setup for this purpose, which detects entangled states with cost effective measurements, and which extends naturally to a tomographically complete measurement for quantum state reconstruction. This latter feature is highly advantageous since it allows experimentalists to perform direct detection of entanglement with only a few measurements, and then, if necessary, to perform quantum state tomography by adding additional measurements and using previous data. Thus, our scheme circumvents the highly non-trivial problem of comparing and connecting standard entanglement witness measurements with those which are useful for state tomography.

Our results also provide other advantages such as offering *double* the efficiency of standard and nonlinear witnesses, with both upper and lower bounds. One consequence of our analysis is that certain sets of MUBs are more 'useful' for entanglement detection than others. For instance, in dimension $d = 4$, the set of 3 MUBs which extends to a complete set provides the minimal (weakest) lower bound and therefore detects a smaller set of entangled states than unextendible MUBs. Thus, one might expect that unextendible MUBs are more useful in other dimensions too. We also note that the results can be generalized to weighted 2-designs [34], which would allow for entanglement detection and state tomography in dimensions where the existence of MUBs and SICs is not yet known.

We envisage directions in entanglement detection beyond standard witnesses and towards related problems in quantum information theory. While we have already shown some links between standard entanglement witnesses and the MUB-inequality (10) and the SIC-inequality (13), we expect further connections to also hold true. For example, recently it has been shown that MUBs can be used to construct positive but not completely positive maps, which lead to a class of entanglement witnesses [35]. Further relations in this direction may reveal additional capabilities of entanglement witnesses at an even deeper level. It would also be interesting to consider nonlinearity, e.g. in [36], to improve the inequalities. We also hope that the presented framework of entanglement detection may offer insightful hints towards a solution of the existence problem for MUBs and SICs from an entanglement perspective [25]. In addition, MUBs and SICs have quite recently been generalized by relaxing the rank-1 condition to so-called mutually unbiased measurements and SIC measurements, which exist in all finite dimensions [37]. Both of these, as well as other similar measurements, could be applied to our framework in similar ways, leading to more experimentally feasible entanglement detection methods in arbitrary dimensions.

Acknowledgments

JB is supported by the ITRC (Information Technology Research Center) support program (IITP-2018-2018-0-01402), the Institute for Information & communications Technology Promotion (IITP) grant funded by the Korea government (MSIP) (R0190-17-2028), National Research Foundation of Korea (NRF-2017R1E1A1A03069961), the KIST Institutional Program (2E26680-17-P025), and the People Programme (Marie Curie Actions) of the European Union Seventh Framework Programme (FP7/2007-2013) under REA grant agreement N 609305. BCH gratefully acknowledges the Austrian Science Fund FWF-P26783. DM has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 663830. The authors are grateful to an anonymous referee for helpful comments.

Appendix A. Quantum 2-Designs, MUBs and SICs

In these appendices we review known results on quantum 2-designs, MUBs, SIC-POVMs, and entanglement witnesses. The main results are presented, including a derivation of the lower and upper bounds for inequalities which detect entangled states via collections of MUBs and SIC vectors. We analyse the capability of our criterion, and show that as we apply more measurements, i.e. as the number of MUBs and SIC vectors increase, the criterion detects larger sets of entangled states. When we apply a quantum 2-design, i.e. a full set of $(d+1)$ MUBs or d^2 SIC vectors, the inequalities provide a necessary and sufficient condition for the separability of a certain class of quantum states, namely the symmetric states. We also show for quantum 2-designs how our detection criterion is related to entanglement witnesses.

Let us begin with a discussion on quantum 2-designs, also known as complex projective 2-designs, and recall two well known examples, a complete set of $(d+1)$ MUBs and a SIC-POVM consisting of d^2 elements. An ensemble of n normalized d-dimensional vectors $\mathcal{D} = \{|\psi_k\rangle\} \subseteq \mathbb{C}^d$ is a quantum 2-design if the average value of any second order polynomial $f(\psi)$ over the set $\mathcal{D}$ is identical to the average of $f(\psi)$ over the unitarily invariant Haar distribution of unit vectors $|\psi\rangle \in \mathbb{C}^d$. To be precise, $f(\psi)$ is a homogenous polynomial of degree two in the coefficients of $|\psi\rangle$ and of degree two in the complex conjugates of these coefficients. In other words, $\mathcal{D}$ is a quantum 2-design if it has the first two moments equal to those of the Haar distribution. It can be shown that such an ensemble of vectors is a quantum 2-design if and only if

$$\frac{1}{n}\sum_{i=1}^{n}|\psi_i\rangle\langle\psi_i|^{\otimes 2} = \frac{2}{d(d+1)}\Pi_{\mathrm{sym}}, \tag{A.1}$$

where Π_{sym} is the projector onto the symmetric subspace of $\mathbb{C}^d \otimes \mathbb{C}^d$.

We write the symmetric and anti-symmetric projectors,

$$\Pi_{\mathrm{sym}} = \frac{1}{2}(\mathbb{1}_d \otimes \mathbb{1}_d + \Pi), \text{ and } \Pi_{\mathrm{asym}} = \frac{1}{2}(\mathbb{1}_d \otimes \mathbb{1}_d - \Pi)$$

respectively, where $\mathbb{1}_d$ denotes the identity operator in d-dimensional Hilbert space, and Π corresponds to the permutation operator in $\mathcal{B}(\mathbb{C}^d \otimes \mathbb{C}^d)$. Note the useful relation that $\Pi^{\Gamma} = d|\Phi^+\rangle\langle\Phi^+|$, with Γ the partial transpose and $|\Phi^+\rangle = \frac{1}{\sqrt{d}}\sum_{i=1}^{d}|ii\rangle$ the maximally entangled state.

Well known examples of quantum 2-designs are complete sets of $(d+1)$ MUBs and SIC-POVMs. Let $\mathcal{B}_k = \{|b_i^k\rangle\}_{i=1}^{d}$ denote an orthonormal basis of the space $\mathbb{C}^d$. $\mathcal{B}_k$ and $\mathcal{B}_{k'}$ are called mutually unbiased if it holds that for all i, i', $|\langle b_i^k|b_{i'}^{k'}\rangle|^2 = d^{-1}$. SIC states are a set of normalized vectors $\{|s_j\rangle\}_{j=1}^{\widetilde{m}}$ in $\mathbb{C}^d$ satisfying the relation $|\langle s_j|s_{j'}\rangle|^2 = (d+1)^{-1}$ for all $j \neq j'$. The SIC states form a SIC-POVM when $\widetilde{m} = d^2$. Suppose that for a d-dimensional Hilbert space, there exist $(d+1)$ MUBs and d^2 SIC states. Then, it holds that

$$\widetilde{\Pi}_{\mathrm{sym}} = \frac{1}{d(d+1)}\sum_{k=1}^{d+1}\sum_{i=1}^{d}|b_i^k\rangle\langle b_i^k|^{\otimes 2} = \frac{1}{d^2}\sum_{j=1}^{d^2}|s_j\rangle\langle s_j|^{\otimes 2},$$

where $\widetilde{\Pi}_{\mathrm{sym}}$ denotes the normalized projection onto the symmetric subspace, $\widetilde{\Pi}_{\mathrm{sym}} = 2[d(d+1)]^{-1}\Pi_{\mathrm{sym}}$.

Note that the existence of a complete set of MUBs and a SIC-POVM has been a long-standing open problem in quantum information theory and is related to several other unsolved problems in mathematics such as orthogonal decompositions of Lie algebras. It is conjectured that there exist $(d+1)$ MUBs if and only if the dimension d is a prime-power, while a set of d^2 SIC vectors is conjectured to exist for all d [38]. So far, it is known that complete sets of MUBs exist in all prime-power dimensions [21, 26–29], while only significantly smaller sets have been found in other composite dimensions. In particular, for dimension $d = 6$, numerical calculations suggest that there exist only 3 MUBs [30]. On the other hand, numerical solutions of SIC-POVMs have been found in all dimensions $d \leqslant 151$ [32, 39], as well as in several higher dimensions [40].

Appendix B. Detecting entangled states using MUBs and SICs

Let us now consider incomplete sets of MUBs and subsets of a SIC-POVM for entanglement detection. We will formulate the inequalities in terms of probabilities, having both upper and lower bounds, which are satisfied by all separable states. Since the structure of MUBs and SICs is not fully understood, it is a non-trivial task to derive these bounds. For instance, in certain dimensions d, different equivalence classes of MUBs exist, and the bounds can often depend on the choice of a particular class. Furthermore, the bounds do not appear to have a simple analytical expression, behaving differently as the dimension changes. In the following, we will first consider entanglement detection with measurements corresponding to MUBs, and then apply similar techniques to derive bounds for SICs. Finally, we show the relationship between quantum 2-designs and entanglement witnesses.

We denote by $I^{(\mathrm{M})}_{m,d}$ and $I^{(\mathrm{S})}_{\widetilde{m},d}$, collections of probabilities when measurements are applied from sets of MUBs and SIC vectors, respectively. For measurements of a set of m MUBs, $\{\mathcal{B}_k\}_{k=1}^{m}$ in $\mathbb{C}^d$, or a set $S_{\widetilde{m}} \subseteq \mathbb{C}^d$ of $\widetilde{m}$ SIC states from a SIC-POVM, applied to each subsystem of a $(d \times d)$ bipartite state ρ, these quantities are defined as,

$$I^{(\mathrm{M})}_{m,d}(\rho\colon \{\mathcal{B}_k\}_{k=1}^{m}) = \sum_{k=1}^{m}\sum_{i=1}^{d} \Pr(i, i|\mathcal{B}_k, \mathcal{B}_k), \tag{B.1}$$

$$I^{(\mathrm{S})}_{\widetilde{m},d}(\rho\colon S_{\widetilde{m}}) = \sum_{j=1}^{\widetilde{m}} \Pr(j, j|S_{\widetilde{m}}, S_{\widetilde{m}}), \tag{B.2}$$

where we have $\Pr(i, i|\mathcal{B}_k, \mathcal{B}_k) = \mathrm{tr}[|b_i^k\rangle\langle b_i^k|\otimes|b_i^k\rangle\langle b_i^k|\,\rho]$ and $\Pr(j, j|S_{\widetilde{m}}, S_{\widetilde{m}}) = \mathrm{tr}[|s_j\rangle\langle s_j|\otimes|s_j\rangle\langle s_j|\,\rho]$. We now derive upper and lower bounds for the quantities $I^{(\mathrm{M})}_{m,d}$ and $I^{(\mathrm{S})}_{\widetilde{m},d}$, which hold true for all separable states.

B.1. Lower and upper bounds of $I^{(\mathrm{M})}_{m,d}$

Let $L^{(\mathrm{M})}_{m,d}$ and $U^{(\mathrm{M})}_{m,d}$ denote the upper and lower bounds of $I^{(\mathrm{M})}_{m,d}$, respectively, for a set of m MUBs, $\{\mathcal{B}_k\}_{k=1}^{m}$, with $1 < m \leqslant d+1$. We calculate these quantities by minimizing and maximizing over all separable states such that

$$L^{(\mathrm{M})}_{m,d}(\{\mathcal{B}_k\}_{k=1}^{m}) = \min_{\sigma_{\mathrm{sep}}} I^{(\mathrm{M})}_{m,d}(\sigma_{\mathrm{sep}}\colon \{\mathcal{B}_k\}_{k=1}^{m}), \tag{B.3}$$

$$U^{(\mathrm{M})}_{m,d}(\{\mathcal{B}_k\}_{k=1}^{m}) = \max_{\sigma_{\mathrm{sep}}} I^{(\mathrm{M})}_{m,d}(\sigma_{\mathrm{sep}}\colon \{\mathcal{B}_k\}_{k=1}^{m}). \tag{B.4}$$

For certain dimensions d, there exists inequivalent sets of m MUBs, up to unitary transformations. For instance, some sets extend to $(d+1)$ MUBs while others are unextendible [41]. Thus, the bounds above may also have a dependence on the choice of MUBs, and hence we also classify these additional bounds as follows

$$L^{-(\mathrm{M})}_{m,d} = \min_{\{\mathcal{B}_k\}_{k=1}^{m}} L^{(\mathrm{M})}_{m,d}(\{\mathcal{B}_k\}_{k=1}^{m}), \tag{B.5}$$

$$L^{+(\mathrm{M})}_{m,d} = \max_{\{\mathcal{B}_k\}_{k=1}^{m}} L^{(\mathrm{M})}_{m,d}(\{\mathcal{B}_k\}_{k=1}^{m}), \tag{B.6}$$

$$U^{-(\mathrm{M})}_{m,d} = \min_{\{\mathcal{B}_k\}_{k=1}^{m}} U^{(\mathrm{M})}_{m,d}(\{\mathcal{B}_k\}_{k=1}^{m}), \tag{B.7}$$

$$U^{+(\mathrm{M})}_{m,d} = \max_{\{\mathcal{B}_k\}_{k=1}^{m}} U^{(\mathrm{M})}_{m,d}(\{\mathcal{B}_k\}_{k=1}^{m}), \tag{B.8}$$

where the minimum and maximum are taken over all possible collections of m MUBs, $\{\mathcal{B}_k\}_{k=1}^{m}$, that exist in dimension d. Note that for $d \leqslant 5$, all sets of MUBs are known [42, 43]. However, for $d \geqslant 6$, the complete classification of MUBs remains an open problem, even for prime-power dimensions, hence such an optimization is currently not possible in large dimensions.

It then follows we have the bounds

$$L^{-(\mathrm{M})}_{m,d} \leqslant L^{+(\mathrm{M})}_{m,d} \leqslant I^{(\mathrm{M})}_{m,d}(\sigma_{\mathrm{sep}}) \leqslant U^{(\mathrm{M})}_{m,d}, \tag{B.9}$$

that are satisfied by all separable states (as visulized in figure B1). We will show in the next section that the upper bound $U^{(\mathrm{M})}_{m,d}$ is independent of the choice of MUBs, i.e. $U^{(\mathrm{M})}_{m,d} = U^{\pm(\mathrm{M})}_{m,d}$. The tighter lower bound, $L^{+(\mathrm{M})}_{m,d}$, applies only for a particular set of MUBs, i.e. the set which maximizes $L^{(\mathrm{M})}_{m,d}$ in equation (B.6). We also note that the minimal lower bound $L^{-(\mathrm{M})}_{m,d}$ applies for any choice of m MUBs. Thus, entangled states are detected by observing violations of $L^{-(\mathrm{M})}_{m,d}$ and $U^{(\mathrm{M})}_{m,d}$ regardless of the choice of MUBs.

B.1.1. Upper bound $U^{(\mathrm{M})}_{m,d}$. In [14] the upper bound has no dependence on the selection of m MUBs and it is shown that

$$U^{(\mathrm{M})}_{m,d} \coloneqq U^{\pm(\mathrm{M})}_{m,d} = 1 + \frac{m-1}{d}. \tag{B.10}$$

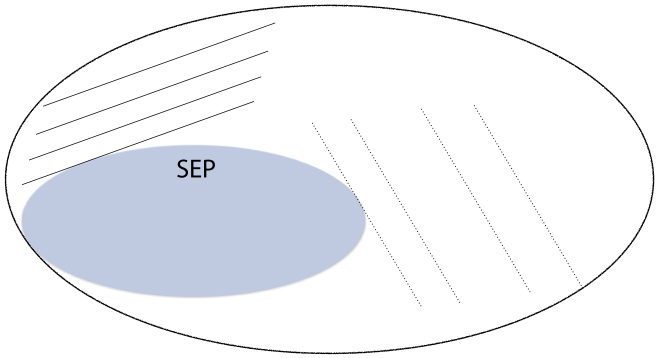

Figure B1. Entanglement detection via MUBs and SICs is illustrated, as shown by the inequalities presented in equations (B.9) and (B.23). Since both the upper and lower bounds are linear with respect to quantum states, they correspond to distinct hyperplanes that separate some entangled states from separable ones. Violation of either bound detect entangled states.

Table B1. Upper bounds $U^{(\mathrm{M})}_{m,d}$ in equation (B.10) are summarized for m MUBs in $\mathbb{C}^d$, for $d = 2, 3, 4$. As the number of MUBs decreases from m to $m-1$, the upper bound is reduced uniformly by $1/d$.

m	$U^{(\mathrm{M})}_{m,2}$	$U^{(\mathrm{M})}_{m,3}$	$U^{(\mathrm{M})}_{m,4}$
2	3/2	4/3	5/4
3	2	5/3	6/4
4		2	7/4
5			2

We note that for $m = d + 1$, i.e. the quantum 2-design case, the upper bound is given by $U^{(\mathrm{M})}_{d+1,d} = 2$ and is clearly independent of the dimension d.

We also observe that removing a single basis from the set of m MUBs decreases the upper bound uniformly by $1/d$, i.e.

$$U^{(\mathrm{M})}_{m+1,d} - U^{(\mathrm{M})}_{m,d} = d^{-1}, \tag{B.11}$$

and the bound is not influenced by which basis is subtracted from the set of MUBs. The bounds for $d = 2, 3, 4$ are summarized in table B1.

B.1.2. Lower bound $L^{(\mathrm{M})}_{m,d}$. For the lower bounds of $I^{(\mathrm{M})}_{m,d}$, the minimization and maximization of equations (B.5) and (B.6) over all MUBs do not coincide in general, i.e. $L^{-(\mathrm{M})}_{m,d} \leqslant L^{+(\mathrm{M})}_{m,d}$. Let us first consider the minimization in equation (B.3) for m MUBs, $\{\mathcal{B}_k\}_{k=1}^m$. Recall that a separable state can be decomposed by a convex combination of product states. This means that it suffices to consider the minimization over only product states, as follows

$$L^{(\mathrm{M})}_{m,d}(\{\mathcal{B}_k\}_{k=1}^m) := \min_{|e\rangle,|f\rangle} \sum_{k=1}^{m}\sum_{i=1}^{d} |\langle b_i^k|e\rangle|^2 |\langle b_i^k|f\rangle|^2, \tag{B.12}$$

where $\mathcal{B}_k = \{|b_i^k\rangle\}_{i=1}^d$, and unit vectors $|e\rangle$, $|f\rangle \in \mathbb{C}^d$. To obtain the minimal and maximal bounds in equations (B.5) and (B.6), the optimization must run over all selections of m MUBs that exist. We do not yet have a systematic method of finding optimal sets of m MUBs that give the tight and minimal lower bounds $L^{+(\mathrm{M})}_{m,d}$ and $L^{-(\mathrm{M})}_{m,d}$. In what follows, we derive these bounds for dimensions $d = 2, 3, 4$.

The property of equivalence classes of MUBs, up to unitary or anti-unitary transformations, is useful to simplify the numerical optimizations in equations (B.5) and (B.6). We call a set of m MUBs, $\{\mathcal{B}_k\}_{k=1}^m$, equivalent to another set of m MUBs, $\{\mathcal{B}'_k\}_{k=1}^m$, denoted by

$$\{\mathcal{B}_k\}_{k=1}^m \sim \{\mathcal{B}'_k\}_{k=1}^m,$$

if there exists a unitary or anti-unitary transformation, denoted by V, such that $\mathcal{B}_k = V\mathcal{B}'_k V^\dagger$ for $k = 1,\ldots,m$. Note that equivalent sets of m MUBs give the same values for $I^{(\mathrm{M})}_{m,d}$:

Table B2. Lower bounds $L_{m,d}^{(\mathrm{M})}$ in equation (B.12) are summarized for m MUBs in $\mathbb{C}^d$, for $d = 2, 3, 4$.

m	$L_{m,2}^{(\mathrm{M})}$	$L_{m,3}^{(\mathrm{M})}$	$L_{m,4}^{-(\mathrm{M})}$	$L_{m,4}^{+(\mathrm{M})}$
2	1/2	0.211..	0	0
3	1	1/2	1/4	1/2
4		1	1/2	1/2
5			1	1

$$\{\mathcal{B}_k\}_{k=1}^m \sim \{\mathcal{B}'_k\}_{k=1}^m \Rightarrow I_{m,d}^{(\mathrm{M})}(\sigma_{\mathrm{sep}}\colon \{\mathcal{B}_k\}_{k=1}^m) = I_{m,d}^{(\mathrm{M})}(\sigma_{\mathrm{sep}}\colon \{\mathcal{B}'_k\}_{k=1}^m). \tag{B.13}$$

The converse, however, does not hold true in general. It therefore suffices to consider distinct equivalence classes in the optimization of equations (B.5) and (B.6).

It turns out that, for dimensions $d = 2, 3$, all sets of m MUBs with $m \leqslant d + 1$ are equivalent. In these low dimensions, the optimization in equations (B.5) and (B.6) is not necessary, and hence, for any m MUBs,

$$L_{m,d}^{(\mathrm{M})} \coloneqq L_{m,d}^{(\mathrm{M})}(\{\mathcal{B}_k\}_{k=1}^m) = L_{m,d}^{\pm(\mathrm{M})}.$$

In table B2, these lower bounds are listed as $L_{2,2}^{(\mathrm{M})} = 1/2$, $L_{2,3}^{(\mathrm{M})} = 0.211\ldots$, and $L_{3,3}^{(\mathrm{M})} = 1/2$. The detailed computation is shown as follows.

In $d = 2$, there is only one pair of MUBs, $\{B_1, B_2\}$, up to equivalence, which can be expressed as a pair of matrices,

$$\mathcal{B}_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ and } \mathcal{B}_2 = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$

where the columns form the basis elements. Hence, for $m = 2$, there is no need to optimize over all pairs of MUBs, and a numerical minimization is applied over all states $|e\rangle = \cos(\theta)|0\rangle + \mathrm{e}^{\mathrm{i}\phi}\sin(\theta)|1\rangle$ and $|f\rangle = \cos(\theta')|0\rangle + \mathrm{e}^{\mathrm{i}\phi'}\sin(\theta')|1\rangle$ in equation (B.12). This gives the bound $L_{2,2}^{(\mathrm{M})} = 1/2$, as shown in table B2. The case $m = 3$, i.e. a quantum 2-design, for which $L_{3,2}^{(\mathrm{M})} = 1$ will be shown later using a connection to entanglement witnesses.

In $d = 3$, the complete set of four MUBs in matrix form are,

$$\mathcal{B}_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},\ \mathcal{B}_2 = \frac{1}{\sqrt{3}}\begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix},$$

$$\mathcal{B}_3 = \frac{1}{\sqrt{3}}\begin{pmatrix} 1 & 1 & 1 \\ \omega & \omega^2 & 1 \\ \omega & 1 & \omega^2 \end{pmatrix},\ \mathcal{B}_4 = \frac{1}{\sqrt{3}}\begin{pmatrix} 1 & 1 & 1 \\ \omega^2 & 1 & \omega \\ \omega^2 & \omega & 1 \end{pmatrix},$$

where the columns form the basis elements. For each $m \leqslant 4$, there exists only one equivalence class of MUBs. That is, $\{\mathcal{B}_1, \mathcal{B}_2\}$ for $m = 2$, and $\{\mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3\}$ when $m = 3$. By performing a minimization of $I_{m,d}^{(\mathrm{M})}(\sigma_{\mathrm{sep}})$ over all normalized states $|e\rangle, |f\rangle \in \mathbb{C}^3$, we obtain the bounds given in table B2.

For $d = 4$, it is no longer true that there is a unique equivalence class of MUBs for each m, thus, we have in general,

$$L_{m,4}^{-(\mathrm{M})} \leqslant L_{m,4}^{+(\mathrm{M})}.$$

For pairs of MUBs, i.e. $m = 2$, there exists a one-parameter family of equivalence classes, denoted by $\mathcal{P}(x) = \{\mathcal{B}_1, \mathcal{B}_2(x)\}$, and for triples of MUBs, i.e. $m = 3$, there exists a three-parameter family of equivalence classes, namely,

$$\mathcal{T}(x, y, z) = \{\mathcal{B}_1, \mathcal{B}_2(x), \mathcal{B}_3(y, z)\}. \tag{B.14}$$

Here, the parameters take the values $x, y, z \in [0, \pi]$, and in matrix form, the bases can be expressed as

$$\mathcal{B}_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},\ \mathcal{B}_2(x) = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & \mathrm{i}\mathrm{e}^{\mathrm{i}x} & -\mathrm{i}\mathrm{e}^{\mathrm{i}x} \\ 1 & -1 & -\mathrm{i}\mathrm{e}^{\mathrm{i}x} & \mathrm{i}\mathrm{e}^{\mathrm{i}x} \end{pmatrix},$$

$$\text{and } \mathcal{B}_3(y, z) = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ -\mathrm{e}^{\mathrm{i}y} & \mathrm{e}^{\mathrm{i}y} & \mathrm{e}^{\mathrm{i}z} & -\mathrm{e}^{\mathrm{i}z} \\ \mathrm{e}^{\mathrm{i}y} & -\mathrm{e}^{\mathrm{i}y} & \mathrm{e}^{\mathrm{i}z} & -\mathrm{e}^{\mathrm{i}z} \end{pmatrix}, \tag{B.15}$$

where the columns correspond to the basis vectors [43]. Then, for $x \neq x'$ the two sets $\mathcal{P}(x)$ and $\mathcal{P}(x')$ are inequivalent. Similarly, the two sets $\mathcal{T}(x,\ y,\ z)$ and $\mathcal{T}(x',\ y',\ z')$ for $(x,\ y,\ z) \neq (x',\ y',\ z')$ are inequivalent. When $m = 2$, it turns out that, nevertheless, all pairs of MUBs provide the same lower bound, i.e. $L_{2,4}^{\pm(\mathrm{M})} \coloneqq L_{2,4}^{(\mathrm{M})}$. However, since $L_{2,4}^{(\mathrm{M})} = 0$, no entangled state can be detected via this bound.

Next, for $m = 3$, the lower bound varies according to our choice of triple $\mathcal{T}(x,\ y,\ z)$. Considering all possible sets of 3 MUBs, we find

$$L_{3,4}^{+(\mathrm{M})} = \max_{x,y,z} L_{3,4}^{(\mathrm{M})}(\mathcal{T}(x,\ y,\ z)) = \frac{1}{2}, \text{ and}$$
$$L_{3,4}^{-(\mathrm{M})} = \min_{x,y,z} L_{3,4}^{(\mathrm{M})}(\mathcal{T}(x,\ y,\ z)) = \frac{1}{4}.$$

These bounds are achieved for the triples $\mathcal{T}(\pi/2,\ 0,\ 0)$ and $\mathcal{T}(\pi/2,\ \pi/2,\ \pi/2)$, respectively. The only triple which extends to a larger set of MUBs is $\mathcal{T}(\pi/2,\ \pi/2,\ \pi/2)$. All other members of the three-parameter family are examples of unextendible MUBs. Hence, the unextendible MUBs detect more entanglement than the extendible triple since they provide tighter lower bounds.

There is only one equivalence class of MUBs for each $m = 4, 5$, given by $\mathcal{T}(\pi/2,\ \pi/2,\ \pi/2) \cup \{B_4\}$ and $\mathcal{T}(\pi/2,\ \pi/2,\ \pi/2) \cup \{B_4,\ B_5\}$, respectively, where,

$$\mathcal{B}_4 = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ \mathrm{i} & -\mathrm{i} & \mathrm{i} & -\mathrm{i} \\ -1 & -1 & 1 & 1 \\ \mathrm{i} & -\mathrm{i} & -\mathrm{i} & \mathrm{i} \end{pmatrix}, \text{ and}$$
$$\mathcal{B}_5 = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ \mathrm{i} & -\mathrm{i} & \mathrm{i} & -\mathrm{i} \\ \mathrm{i} & -\mathrm{i} & -\mathrm{i} & \mathrm{i} \\ -1 & -1 & 1 & 1 \end{pmatrix}. \tag{B.16}$$

Thus, since it is not necessary to optimize over collections of MUBs, we perform a minimization over product states to find $L_{4,4}^{(\mathrm{M})} = 1/2$ and $L_{5,4}^{(\mathrm{M})} = 1$. These bounds, including the case $m = 4$, are summarized in table B2.

B.2. Lower and upper bounds on $I_{\widetilde{m},d}^{(\mathrm{S})}$

We now consider measurements using SIC states to construct similar inequalities for $I_{\widetilde{m},d}^{(\mathrm{S})}$ defined in equation (B.2). It is important to specify which SIC-POVM S_d^2 we use for our measurements, as for a given dimension d they are usually not unique. Hence, the bounds we derive will depend explicitly on the given SIC-POVM.

For a subset of $\widetilde{m}$ SIC vectors, $S_{\widetilde{m}} = \{|s_j\rangle\}_{j=1}^{\widetilde{m}} \subseteq S_{d^2}$ with $\widetilde{m} \leqslant d^2$, let $U_{\widetilde{m},d}^{(\mathrm{S})}$ and $L_{\widetilde{m},d}^{(\mathrm{S})}$ denote the upper and lower bounds,

$$L_{\widetilde{m},d}^{(\mathrm{S})}(S_{\widetilde{m}}) = \min_{\sigma_{\mathrm{sep}}} I_{m,d}^{(\mathrm{S})}(\sigma_{\mathrm{sep}} : S_{\widetilde{m}}), \tag{B.17}$$
$$U_{\widetilde{m},d}^{(\mathrm{S})}(S_{\widetilde{m}}) = \max_{\sigma_{\mathrm{sep}}} I_{m,d}^{(\mathrm{S})}(\sigma_{\mathrm{sep}} : S_{\widetilde{m}}). \tag{B.18}$$

Since the lower and upper bounds may depend on which subset of $\widetilde{m}$ states are taken from the SIC-POVM S_d^2, let us introduce maximal and minimal bounds optimized over $\widetilde{m}$ collections of SIC vectors, as follows,

$$L_{\widetilde{m},d}^{-(\mathrm{S})} = \min_{S_{\widetilde{m}} \subseteq S_{d^2}} L_{\widetilde{m},d}^{(\mathrm{S})}(S_{\widetilde{m}}), \tag{B.19}$$
$$L_{\widetilde{m},d}^{+(\mathrm{S})} = \max_{S_{\widetilde{m}} \subseteq S_{d^2}} L_{\widetilde{m},d}^{(\mathrm{S})}(S_{\widetilde{m}}), \tag{B.20}$$
$$U_{\widetilde{m},d}^{-(\mathrm{S})} = \min_{S_{\widetilde{m}} \subseteq S_{d^2}} U_{\widetilde{m},d}^{(\mathrm{S})}(S_{\widetilde{m}}), \tag{B.21}$$
$$U_{\widetilde{m},d}^{+(\mathrm{S})} = \max_{S_{\widetilde{m}} \subseteq S_{d^2}} U_{\widetilde{m},d}^{(\mathrm{S})}(S_{\widetilde{m}}), \tag{B.22}$$

where S_d^2 is a given SIC-POVM in dimension d. Note that these optimizations can only be applied when the explicit form of the SIC-POVM is known, which is not the case in large dimensions. As shown below, it turns out that $I_{\widetilde{m},d}^{(\mathrm{S})}$ satisfies the inequalities,

$$L_{\widetilde{m},d}^{-(\mathrm{S})} \leqslant L_{\widetilde{m},d}^{+(\mathrm{S})} \leqslant I_{\widetilde{m},d}^{(\mathrm{S})}(\sigma_{\mathrm{sep}}) \leqslant U_{\widetilde{m},d}^{-(\mathrm{S})} \leqslant U_{\widetilde{m},d}^{+(\mathrm{S})}, \tag{B.23}$$

for all separable states σ_{sep}. Entangled states are detected by violations of these inequalities. The tighter bounds only apply for a specific subset of SIC vectors, i.e. the set $S_{\widetilde{m}} \subseteq S_{d^2}$ used to find $L_{\widetilde{m},d}^{+(\mathrm{S})}$ or $U_{\widetilde{m},d}^{-(\mathrm{S})}$ in equations (B.20) and (B.21). The weaker bounds apply for any subset of $\widetilde{m}$ states chosen from a particular SIC-POVM.

For the optimizations in equations (B.17) and (B.18) over separable states, it suffices to consider only product states due to the convexity of the set of separable states. Hence, given a set $S_{\widetilde{m}}$ of $\widetilde{m}$ SIC vectors

$$L^{(\mathrm{S})}_{\widetilde{m},d}(S_{\widetilde{m}}) = \min_{|e\rangle,|f\rangle} \sum_{|s_j\rangle\in S_{\widetilde{m}}} |\langle s_j|e\rangle|^2 |\langle s_j|f\rangle|^2, \tag{B.24}$$

$$U^{(\mathrm{S})}_{\widetilde{m},d}(S_{\widetilde{m}}) = \max_{|e\rangle} \sum_{|s_j\rangle\in S_{\widetilde{m}}} |\langle s_j|e\rangle|^4, \tag{B.25}$$

where $|e\rangle, |f\rangle \in \mathbb{C}^d$. We have not yet found a systematic method to find these minimal and maximal bounds in general. In the following we derive the bounds for $d = 2, 3$ and optimize over all subsets of $\widetilde{m}$ SIC vectors from a given SIC-POVM. However, for $d = 4$, we only find suboptimal bounds.

B.2.1. Upper bounds $U^{(\mathrm{S})}_{\widetilde{m},d}$. As previously mentioned, the bounds we derive will depend explicitly on the given SIC-POVM. Here, we will only consider Heisenberg–Weyl SICs which are constructed from the Heisenberg–Weyl group, generated by the phase and cyclic shift operators (modulo d), which are defined as

$$Z|j\rangle = \omega^j |j\rangle, \quad X|j\rangle = |j+1\rangle, \tag{B.26}$$

where $\omega = \mathrm{e}^{2\pi \mathrm{i}/d}$ and $\{|j\rangle\}_{j=0}^{d-1}$ is the standard basis of $\mathbb{C}^d$. A Heisenberg–Weyl SIC can then be constructed by taking the orbit of a fiducial vector $|\psi_f\rangle$, i.e.

$$|s_{a,b}\rangle = \mathrm{e}^{-\mathrm{i}ab\pi/d} X^a Z^b |\psi_f\rangle, \tag{B.27}$$

for $a, b = 0,\ldots, d-1$.

For dimension $d = 2$, there exist two SIC-POVMs, which are related via complex conjugation [13, 38]. Since the bounds are invariant under complex conjugation we are free to choose either SIC without it affecting our results. One of the SIC-POVMs is generated by the fiducial vector

$$|\psi_f\rangle = \frac{1}{\sqrt{6}}(\sqrt{3+\sqrt{3}}\,|0\rangle + \mathrm{e}^{\pi\mathrm{i}/4}\sqrt{3-\sqrt{3}}\,|1\rangle).$$

The resulting POVM can be written more simply in terms of the four vectors

$$\begin{aligned}
|s_1\rangle &= |0\rangle,\\
|s_2\rangle &= \frac{1}{\sqrt{3}}(|0\rangle + \sqrt{2}\,|1\rangle),\\
|s_3\rangle &= \frac{1}{\sqrt{3}}(\mathrm{e}^{-\frac{\mathrm{i}\pi}{3}}|0\rangle + \sqrt{2}\,\mathrm{e}^{\frac{\mathrm{i}\pi}{3}}|1\rangle),\\
|s_4\rangle &= \frac{1}{\sqrt{3}}(\mathrm{e}^{\frac{\mathrm{i}\pi}{3}}|0\rangle + \sqrt{2}\,\mathrm{e}^{-\frac{\mathrm{i}\pi}{3}}|1\rangle),
\end{aligned} \tag{B.28}$$

where $\{|0\rangle, |1\rangle\}$ is the standard basis of $\mathbb{C}^2$. The states, which form a quantum 2-design, also form a tetrahedron in the Bloch sphere. It turns out that the upper bounds we calculate do not depend on which choice of $\widetilde{m}$ SIC vectors from equation (B.28) we take. In particular, for both $\widetilde{m} = 2, 3$, the two bounds $U^{-(\mathrm{S})}_{\widetilde{m},d}$ and $U^{+(\mathrm{S})}_{\widetilde{m},d}$ coincide, i.e. $U^{-(\mathrm{S})}_{\widetilde{m},d} = U^{+(\mathrm{S})}_{\widetilde{m},d}$. For $\widetilde{m} = 2$, the upper bound for any pair of SIC vectors is

$$U^{-(\mathrm{S})}_{2,2} = U^{+(\mathrm{S})}_{2,2} = \frac{1}{6}(\sqrt{3}+1)^2. \tag{B.29}$$

For $\widetilde{m} = 3$, any subset of three SIC vectors taken from equation (B.28) gives

$$U^{-(\mathrm{S})}_{3,2} = U^{+(\mathrm{S})}_{3,2} = \frac{4}{3}. \tag{B.30}$$

We note that it is also possible to find the vector $|e\rangle$ in equation (B.25) which attains these bounds. For example, given the set $\{|s_1\rangle, |s_3\rangle\}$, then $|e_{\max}\rangle = \kappa(|s_1\rangle + \mathrm{e}^{\pi\mathrm{i}/3}|s_3\rangle)$, where κ is a normalization factor. In fact, in all of the dimensions we investigate, given a set of $\widetilde{m}$ SIC vectors, $\{|s_j\rangle\}$, the vector achieving the maximum takes the form $|e_{\max}\rangle = \kappa(\sum_j \mathrm{e}^{\pi\mathrm{i}\lambda_j}|s_j\rangle)$, where the summation is taken over all SIC vectors from the set $\{|s_j\rangle\}$.

Now we move to dimension $d = 3$, and use the Hesse SIC [13, 38], which is generated by the Heisenberg–Weyl group from the fiducial vector

$$|\psi_f\rangle = \frac{1}{\sqrt{2}}(|1\rangle - |2\rangle). \tag{B.31}$$

We have chosen the Hesse SIC (which is derived from the Hesse configuration in design theory) due to its special symmetry properties, which are unique among the infinite family of qutrit SIC-POVMs that exist [44]. However, other SIC-POVMs such as the Norrell states would also be interesting to analyse [45, 46]. Written explicitly, the nine SIC vectors are

$$
\begin{aligned}
|s_1\rangle &= \frac{1}{\sqrt{2}}(|1\rangle - |2\rangle),\\
|s_2\rangle &= \frac{1}{\sqrt{2}}(-|0\rangle + |2\rangle),\\
|s_3\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle),\\
|s_4\rangle &= \frac{1}{\sqrt{2}}(\omega|1\rangle - \omega^2|2\rangle),\\
|s_5\rangle &= \frac{1}{\sqrt{2}}(-\omega|0\rangle + |2\rangle),\\
|s_6\rangle &= \frac{1}{\sqrt{2}}(\omega^2|0\rangle - |1\rangle),\\
|s_7\rangle &= \frac{1}{\sqrt{2}}(\omega^2|1\rangle - \omega|2\rangle),\\
|s_8\rangle &= \frac{1}{\sqrt{2}}(-\omega^2|0\rangle + |2\rangle),\\
|s_9\rangle &= \frac{1}{\sqrt{2}}(\omega|0\rangle - |1\rangle),
\end{aligned}
\tag{B.32}
$$

where $\omega = \exp(2\pi \mathrm{i}/3)$ and $\{|0\rangle, |1\rangle, |2\rangle\}$ is the standard basis of $\mathbb{C}^3$.

In contrast to $d = 2$, here we find that the two bounds $U^{-(\mathrm{S})}_{\widetilde{m},d}$ and $U^{+(\mathrm{S})}_{\widetilde{m},d}$ do not in general coincide. We calculate the bound $U^{(\mathrm{S})}_{\widetilde{m},d}(S_{\widetilde{m}})$ in equation (B.18) for all subsets of $\widetilde{m}$ SIC vectors from the 9 vectors in equation (B.32), and find that for each $\widetilde{m}$ there are at most two different bounds. Thus, the smallest of the two bounds must coincide with $U^{-(\mathrm{S})}_{\widetilde{m},d}$, while the largest must coincide with $U^{+(\mathrm{S})}_{\widetilde{m},d}$.

When $\widetilde{m} = 3$, we find two upper bounds for $U^{(\mathrm{S})}_{\widetilde{m},d}(S_{\widetilde{m}})$ depending on our choice of three SIC vectors, $\{|s_i\rangle, |s_j\rangle, |s_k\rangle\}$, from equation (B.32). Denoting this set by the indices (i, j, k), we find that $(1, 2, 3)$, $(1, 4, 7)$, $(1, 5, 9)$, $(1, 6, 8)$, $(2, 4, 9)$, $(2, 5, 8)$, $(2, 6, 7)$, $(3, 4, 8)$, $(3, 5, 7)$, $(3, 6, 9)$, $(4, 5, 6)$ and $(7, 8, 9)$, give an upper bound of $9/8$. The remaining sets give a numerical upper bound of 1.254 14. Thus, the values of $U^{+(\mathrm{S})}_{\widetilde{3},3}$ and $U^{+(\mathrm{S})}_{\widetilde{3},3}$ are given by

$$U^{+(\mathrm{S})}_{\widetilde{3},3} = 1.254\,14\ldots, \tag{B.33}$$

and

$$U^{-(\mathrm{S})}_{\widetilde{3},3} = 9/8. \tag{B.34}$$

We note that the 12 index sets which yield the bound $9/8$ exhibit an interesting property relating to the linear dependencies of the Hesse SIC states. The Hesse configuration is a set of nine vectors and 12 two-dimensional subspaces, where each subspace contains three vectors and each vector appears in four of the subspaces [47]. Rather surprisingly, these two-dimensional subspaces correspond exactly to the 12 sets of three vectors given by the index sets found above [46, 48]. In fact it is this linear dependency that causes the upper bound to take the value $9/8$ in these 12 cases. If the choice of three vectors forms a linearly independent set, which is true in all other cases, the bound takes the larger value.

For $\widetilde{m} = 4$, we also find that the minimal and maximal bounds do not coincide, although all subset of 4 SIC vectors give one of two possible bounds. For example, the set $\{|s_1\rangle, |s_2\rangle, |s_3\rangle, |s_4\rangle\}$ gives the bound

$$U^{-(\mathrm{S})}_{4,3} = 1.25414\ldots, \tag{B.35}$$

while from the set $\{|s_1\rangle, |s_2\rangle, |s_4\rangle, |s_5\rangle\}$ we have,

$$U^{+(\mathrm{S})}_{4,3} = 1.39952\ldots \tag{B.36}$$

When $\widetilde{m} = 5$, two upper bounds for equation (B.18) also exist for all combinations of five SIC vectors. For example, $\{|s_i\rangle\}_{i=1}^{5}$ gives the bound

$$U^{+(\mathrm{S})}_{5,3} = 1.46301\ldots, \tag{B.37}$$

while for the set $\{|s_1\rangle, |s_2\rangle, |s_3\rangle, |s_4\rangle, |s_7\rangle\}$ we have,

$$U^{-(\mathrm{S})}_{5,3} = 1.39952\ldots \tag{B.38}$$

For $\widetilde{m} = 6$, again there are two distinct upper bounds for all combination of six SIC vectors. For example, $\{|s_i\rangle\}_{i=1}^{6}$ gives

Table B3. Lower and upper bounds $L^{(S)}_{\widetilde{m},2}$ and $U^{(S)}_{\widetilde{m},2}$ are shown for $\widetilde{m} = 2, 3, 4$ in dimensions $d = 2$. When $\widetilde{m}$ SIC vectors are chosen from a set of d^2 states, there are $4!(\widetilde{m}!\ (4-\widetilde{m})!)^{-1}$ possible subsets of $\widetilde{m}$ SIC states. It turns out that for $d = 2$, these bounds do not depend on the selection of $\widetilde{m}$ states.

$\widetilde{m}$ SICs	$L^{(S)}_{\widetilde{m},2}$	$U^{(S)}_{\widetilde{m},2}$
2	0	$(\sqrt{3}+1)^2/6$
3	4/15	4/3
4	2/3	4/3

$$U^{+(S)}_{6,3} = \frac{3}{2}, \tag{B.39}$$

and for $\{|s_1\rangle, |s_2\rangle, |s_3\rangle, |s_4\rangle, |s_5\rangle, |s_7\rangle\}$ we have

$$U^{-(S)}_{6,3} = 1.481\ 75\ldots \tag{B.40}$$

When $\widetilde{m} = 7$, the two bounds coincide for all subsets of 7 SIC vectors such that

$$U^{-(S)}_{7,3} = U^{+(S)}_{7,3} = \frac{3}{2}. \tag{B.41}$$

Finally, for $\widetilde{m} = 8$, any set of 8 SIC vectors yields the same bound, hence,

$$U^{-(S)}_{8,3} = U^{+(S)}_{8,3} = \frac{3}{2}. \tag{B.42}$$

Next, for dimension $d = 4$, we choose the SIC-POVM generated from the fiducial vector

$$|\psi_f\rangle = \frac{1}{2\sqrt{3+\Gamma}}(\alpha_+|0\rangle + \beta_+|1\rangle + \alpha_-|2\rangle + \beta_-|3\rangle), \tag{B.43}$$

where $\alpha_\pm = 1 \pm e^{-i\pi/4}$, $\beta_\pm = e^{i\pi/4} \pm i\Gamma^{-3/2}$, and $\Gamma = (\sqrt{5}-1)/2$ is the golden ratio [13, 38]. We have tested several possible subsets $S_{\widetilde{m}}$ for each $\widetilde{m}$ and found that the bound $U^{(S)}_{\widetilde{m},d}(S_{\widetilde{m}})$ in equation (B.23) takes a number of different values depending on the set $S_{\widetilde{m}}$. Let $|s_{a,b}\rangle \in \mathbb{C}^4$ be the SIC states defined in equation (B.27) generated by the fiducial vector of equation (B.43). Choosing the set $S_{\widetilde{m}}$ as the sets $\{|s_{0,0}\rangle, |s_{0,1}\rangle, |s_{0,2}\rangle\}$, $\{|s_{0,0}\rangle, |s_{0,1}\rangle, |s_{0,2}\rangle, |s_{0,3}\rangle\}$, $\{|s_{0,0}\rangle, |s_{0,1}\rangle, |s_{0,2}\rangle, |s_{0,3}\rangle, |s_{1,0}\rangle\}$, etc, for $\widetilde{m} = 3, 4, 5, \ldots$, we present the suboptimal bounds $U^{(S)}_{\widetilde{m},d}(S_{\widetilde{m}})$ in table B5.

B.2.2. Lower bounds $L^{(S)}_{\widetilde{m},d}$. We now apply similar techniques to calculate the lower bound of equation (B.24) for $I^{(S)}_{\widetilde{m},d}$. We will use the same SIC-POVMs as defined in the previous section. For dimensions $d = 2$ we find that $L^{+(S)}_{\widetilde{m},2} = L^{-(S)}_{\widetilde{m},2}$ for all $\widetilde{m} = 2, 3, 4$, hence the bounds in table B3 are both optimal and apply for any choice of SIC vectors.

For $d = 3$ and $\widetilde{m} = 0, \ldots, 5$ we find that $L^{-(S)}_{\widetilde{m},d} = L^{+(SIC)}_{\widetilde{m},d} = 0$. When $\widetilde{m} = 6$, we have

$$L^{-(S)}_{6,3} = 0, \tag{B.44}$$

and

$$L^{+(S)}_{6,3} = 0.112\ 3. \tag{B.45}$$

In fact, for any choice of 6 from the nine SIC vectors in equations (B.32), the lower bound is either 0 or 0.1123. For example, given the set $S_{\widetilde{m}} = \{|s_i\rangle\}_{i=1}^6$, we obtain $L^{(S)}_{6,3}(S_{\widetilde{m}}) = 0$, while for $S_{\widetilde{m}} = \{|s_1\rangle, |s_2\rangle, |s_3\rangle, |s_4\rangle, |s_5\rangle, |s_7\rangle\}$ we have $L^{(S)}_{6,3}(S_{\widetilde{m}}) = 0.112\ 3$.

For $\widetilde{m} = 7$, the bounds are independent of the choice of SIC vectors and attain the value $L^{-(S)}_{\widetilde{m},d} = L^{+(S)}_{\widetilde{m},d} = 0.15$. Finally, for $\widetilde{m} = 8$ the bounds take the value $L^{\pm(S)}_{\widetilde{m},d} = 0.375$.

In dimension $d = 4$, suboptimal lower bounds are presented in table B5 using the same sets of SIC vectors as the upper bounds, i.e. $\{|s_{0,0}\rangle, |s_{0,1}\rangle, |s_{0,2}\rangle\}$, $\{|s_{0,0}\rangle, |s_{0,1}\rangle, |s_{0,2}\rangle, |s_{0,3}\rangle$ etc, for $\widetilde{m} = 3, 4, \ldots$

Table B4. In dimension $d = 3$, we use the Hesse SIC-POVM defined by the 9 SIC vectors of equation (B.32). Both the lower and upper bounds depend on the choice of $\widetilde{m}$ SIC states, although when m is large the upper bounds become independent of the choice and number of SIC vectors. The minimal and maximal bounds of $L^{\pm(\mathrm{S})}_{\widetilde{m},d}$ and $U^{\pm(\mathrm{S})}_{\widetilde{m},d}$ are shown for $\widetilde{m} = 3, 4, 5, 6, 7, 8, 9$, some of which are obtained numerically.

$\widetilde{m}$ SICs	$L^{-(\mathrm{S})}_{\widetilde{m},3}$	$L^{+(\mathrm{S})}_{\widetilde{m},3}$	$U^{+(\mathrm{S})}_{\widetilde{m},3}$	$U^{-(\mathrm{S})}_{\widetilde{m},3}$
3	0	0	1.254 14...	9/8
4	0	0	1.399 52...	1.254 14...
5	0	0	1.463 01...	1.399 52...
6	0	0.1123	3/2	1.481 75...
7	3/20	3/20	3/2	3/2
8	3/8	3/8	3/2	3/2
9	3/4	3/4	3/2	3/2

Table B5. For $\widetilde{m}$ SIC states in $\mathbb{C}^4$, suboptimal lower and upper bounds, denoted by $L^{(\mathrm{S})}_{\widetilde{m},4}(S_{\widetilde{m}})$ and $U^{(\mathrm{S})}_{\widetilde{m},4}(S_{\widetilde{m}})$, are presented, for the quantity $I^{(\mathrm{S})}_{\widetilde{m},4}$. These bounds are satisfied for all separable states, provided a *specific* subset $S_{\widetilde{m}}$ of $\widetilde{m}$ SIC vectors is chosen from the SIC-POVM generated by the fiducial vector of equation (B.43). The subsets we apply are given below equation (B.43).

$\widetilde{m}$ SICs	$L^{(\mathrm{S})}_{\widetilde{m},4}(S_{\widetilde{m}})$	$U^{(\mathrm{S})}_{\widetilde{m},4}(S_{\widetilde{m}})$
3	0	1.1476
4	0	1.2676
5	0	1.3766
6	0	1.4521
7	0.0067	1.4723
8	0.0279	1.4902
9	0.0325	1.5556
10	0.0693	1.5763
11	0.0719	1.5881
12	0.1436	1.5935
13	0.2031	1.6
14	0.2285	1.6
15	0.4363	1.6
16	4/5	1.6

Appendix C. On the capability of detecting entangled states

To summarize, we have derived inequalities given in equations (B.9) and (B.23), for sets of MUBs and subsets of d^2 SIC vectors, respectively. First, for *any* set of m MUBs in dimension d, the quantity $I^{(\mathrm{M})}_{m,d}$ is bounded above and below, for all separable states, by

$$L^{-(\mathrm{M})}_{m,d} \leqslant I^{(\mathrm{M})}_{m,d}(\sigma_{\mathrm{sep}}) \leqslant 1 + \frac{m-1}{d}, \tag{C.1}$$

where the values $L^{-(\mathrm{M})}_{m,d}$ are given in table B2 for $d = 2, 3, 4$. Note that $L^{-(\mathrm{M})}_{m,d} = L^{(\mathrm{M})}_{m,d}$ for $d = 2, 3$, due to the existence of only one equivalence class of m MUBs. We also provide a tighter lower bound $L^{+(\mathrm{M})}_{m,d}$ when $d = 4$, which only holds true if we restrict the choice of MUBs to a specific set. When $m = 3$, this triple of MUBs is given by $\mathcal{T}(\pi/2, \pi/2, \pi/2) \in \mathcal{T}(x, y, z)$, as defined in equation (B.14). From an experimental perspective, this triple of MUBs is more useful for entanglement detection since it detects a larger set of entangled states than any other member of the family $\mathcal{T}(x, y, z)$.

The situation is more complicated for SICs. First we must specify which SIC-POVM we apply in dimension d. We then show in dimensions $d = 2, 3$, that for *any* subset of $\widetilde{m}$ SIC vectors, the quantity $I^{(\mathrm{S})}_{\widetilde{m},d}$ is bounded above and below, for all separable states, by

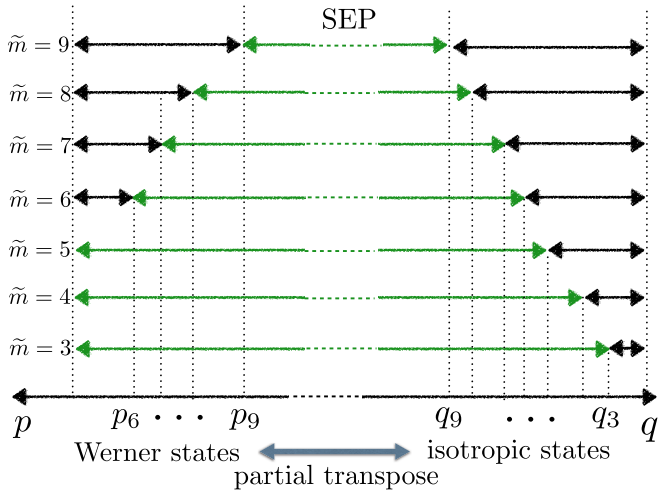

Figure C1. Inequalities for $I^{(S)}_{2,3}$, $I^{(S)}_{3,3}$, and $I^{(S)}_{4,3}$ are applied to detect the entangled Werner and isotropic states defined in equations (C.7) and (C.8). The upper ($U^{-(S)}_{\widetilde{m},d}$) and lower ($L^{+(S)}_{\widetilde{m},d}$) bounds can be found in table B4. Green coloured lines show the range of states satisfying the inequalities, including all separable states. Lower bounds are violated by entangled Werner states and upper bounds by entangled isotropic states, with the critical values for the parameter p and q given as: $p_6 = 0.11$, $p_7 = 0.13$, $p_8 = 0.28$, $p_9 = 0.5$, $q_3 = 1.19$, $q_4 = 0.91$, $q_5 = 0.76$, $q_6 = 0.61$, $q_7 = 0.46$, $q_8 = 0.34$, and $q_9 = 0.25$.

$$L^{-(S)}_{\widetilde{m},d} \leqslant I^{(S)}_{\widetilde{m},d}(\sigma_{\text{sep}}) \leqslant U^{+(S)}_{\widetilde{m},d}, \tag{C.2}$$

where the values $L^{-(S)}_{\widetilde{m},d}$ and $U^{+(S)}_{\widetilde{m},d}$ are given in tables B3 and B4, for dimensions $d = 2, 3$, respectively. Note that in $d = 2$, $L^{-(S)}_{\widetilde{m},d} = L^{(S)}_{\widetilde{m},d}$ and $U^{+(S)}_{\widetilde{m},d} = U^{(S)}_{\widetilde{m},d}$. For $d = 3$ we can derive tighter upper and lower bounds

$$L^{+(S)}_{\widetilde{m},3} \leqslant I^{(S)}_{\widetilde{m},3}(\sigma_{\text{sep}}) \leqslant U^{-(S)}_{\widetilde{m},3}, \tag{C.3}$$

as summarized in table B4. However, equation (C.3) only applies for a specific set of $\widetilde{m}$ SIC vectors, which we have specified explicitly in the derivations above. For $d = 4$ we are unable to find upper and lower bounds which apply for *any* subset of $\widetilde{m}$ SIC vectors, however, we do find suboptimal bounds which apply for a specified set of $\widetilde{m}$ SIC vectors, namely

$$L^{0(S)}_{\widetilde{m},d} \leqslant I^{(S)}_{\widetilde{m},d}(\sigma_{\text{sep}}) \leqslant U^{0(S)}_{\widetilde{m},d}, \tag{C.4}$$

where the bounds are given in table B5. To apply these bounds experimentally, it is required that the measurements correspond to the specified set of SIC vectors.

We will also prove later that for a complete set of $(d + 1)$ MUBs and d^2 SIC vectors, which correspond to quantum 2-designs, the bounds simplify to

$$1 \leqslant I^{(M)}_{d+1,d}(\sigma_{\text{sep}}) \leqslant 2, \tag{C.5}$$

and

$$\frac{d}{d+1} \leqslant I^{(S)}_{d^2,d}(\sigma_{\text{sep}}) \leqslant \frac{2d}{d+1}. \tag{C.6}$$

We now show that the inequalities above, for $I^{(M)}_{m,d}$ and $I^{(S)}_{\widetilde{m},d}$, detect a larger set of entangled states as the number of measurements m increases. In particular, we highlight the following result:

Remark 1. As more MUBs and SIC vectors are applied to the detection criterion, the stronger the capability of detecting entangled states.

For a graphical illustration of this phenomenon we refer the reader to figures 2 and C1.

C.1. Examples: symmetric states

To demonstrate the observation made in remark 1, we consider a particular class of bipartite $(d \times d)$-dimensional quantum states, the so-called symmetric states, and analyse their behaviour with respect to our detection criterion. The first set of states we investigate are the Werner states

$$\rho_{\mathrm{W}}(p) = p\frac{2}{d(d+1)}\Pi_{\mathrm{sym}} + (1-p)\frac{2}{d(d-1)}\Pi_{\mathrm{asym}}, \tag{C.7}$$

where $p \in [0, 1]$. Werner states are separable for $p \geqslant 1/2$ and entangled if $p < 1/2$. We also consider the bipartite isotropic states which are invariant under $U \otimes U^*$

$$\rho_{\mathrm{iso}}(q) = q|\Phi^+\rangle\langle\Phi^+| + (1-q)\frac{\mathbb{1}\otimes\mathbb{1}}{d^2}, \tag{C.8}$$

where $q \in [0, 1]$ and $|\Phi^+\rangle$ denotes a maximally entangled state. Isotropic states are entangled if and only if $q > 1/(d+1)$. Both of these symmetric states are non-positive under the partial transpose if and only if they are entangled. If they are separable, Werner states can be converted to isotropic states, and vice versa, by the partial transpose.

In [14], it is shown that an isotropic state is entangled if and only if it violates the upper bound in equation (C.5). For the Werner states defined in equation (C.7), it is straightforward to compute the following

$$I^{(\mathrm{M})}_{m,d}(\rho_{\mathrm{W}}(p)) = \sum_{k=1}^{m}\sum_{i=1}^{d}\Pr(i,\, i|\mathcal{B}_k,\, \mathcal{B}_k) = \frac{2pm}{d+1}, \tag{C.9}$$

where we note that $\Pr(i,\, i|\mathcal{B}_k,\, \mathcal{B}_k) = 2p(d+1)^{-1}$. For $m = d+1$, we have $I^{(\mathrm{M})}_{d+1,d}(\rho_{\mathrm{W}}(p)) = 2p$. From equation (C.5), it follows that the Werner states $\rho_W(p)$ violate the lower bound if $p < 1/2$, and hence the criterion coincides with the exact separability conditions. We also remark that the upper bound from equation (C.5) has been used to detect bound entangled states [19].

In figure 2, the inequalities of equation (C.1) for $I^{(\mathrm{M})}_{2,3}$, $I^{(\mathrm{M})}_{3,3}$, and $I^{(\mathrm{M})}_{4,3}$ are applied to detect entangled Werner and isotropic states in dimension $d = 3$. It is shown that as m decreases, i.e. as fewer MUBs are measured, the range of the entangled states detected becomes smaller.

For SICs, it is also straightforward to compute the following quantities

$$I^{(\mathrm{S})}_{\widetilde{m},d}(\rho_{\mathrm{W}}(p)) = \frac{2p\widetilde{m}}{d(d+1)}, \tag{C.10}$$

$$I^{(\mathrm{S})}_{\widetilde{m},d}(\rho_{\mathrm{iso}}(q)) = \frac{\widetilde{m}}{d^2}(q(d-1)+1), \tag{C.11}$$

for Werner and isotropic states. We can then determine for which parameters the states satisfy the inequalities in equation (C.6). When $\widetilde{m} = d^2$, it follows that the upper bound in equation (C.6) is violated by all entangled isotropic states, and the lower bound by all entangled Werner states, that is, for $q > 1/(d+1)$ and $p < 1/2$, respectively. Thus, $I^{(\mathrm{S})}_{d^2,d}$ tightly characterizes entangled Werner and isotropic states.

The inequalities given in equations (C.3) and (C.4) with $\widetilde{m} < d^2$ are applied to detect entangled states as follows. Given $\widetilde{m}$, and the values of $I^{(\mathrm{S})}_{\widetilde{m},d}$ from equations (C.10) and (C.11), a violation of either equations (C.3) and (C.4) implies the states are entangled. Critical values of p and q that lead to violations of the inequality (C.4) for $d = 3$ are shown in figure C1, and are denoted by $L_{\widetilde{m}}$ and $U_{\widetilde{m}}$, respectively. One can naturally expect that a larger value of $\widetilde{m}$ implies a higher capability of detecting entangled states, as is indicated in the figure.

Appendix D. Relations: entanglement witnesses and quantum 2-designs

In the following, we summarize the relationship between entanglement witnesses and the structural physical approximation of an entanglement witness. Both an entanglement witness and its structural physical approximation are equivalent in the sense that they detect the same set of entangled states. In particular, we show that when the structural physical approximation is applied to a witness constructed by the partial transpose, the resulting operator coincides with a quantum 2-design. Furthermore, we derive the upper and lower bounds of $I^{(\mathrm{M})}_{m,d}$ and $I^{(\mathrm{S})}_{\widetilde{m},d}$ for a full set of MUBs and SIC vectors, respectively.

D.1. Entanglement witnesses and their equivalent construction

Let $\mathcal{B}(\mathcal{H})$ denote the set of bounded operators in the Hilbert space $\mathcal{H}$. A Hermitian operator $W \in \mathcal{B}(\mathcal{H}\otimes\mathcal{H})$ is an entanglement witness if it satisfies

$$\begin{aligned} &\mathrm{tr}[W\sigma_{\mathrm{sep}}] \geqslant 0, \quad \text{for all separable states } \sigma_{\mathrm{sep}},\\ &\mathrm{tr}[W\rho] < 0, \quad \text{for some entangled states } \rho. \end{aligned} \tag{D.1}$$

Entanglement witnesses can be realized with POVMs. Given a witness W, one can find its decomposition

$$W = \sum_{i=1}^{n} c_i\, M_i, \tag{D.2}$$

for some $n > 1$, with POVM elements $\{M_i\}_{i=1}^n$. If this does not form a resolution of the identity operator, i.e. $\sum_{i=1}^n M_i < I$, then let M_0 denote the positive-operator $M_0 = I - \sum_{i=1}^n M_i$ such that one can construct a complete measurement $\{M_i\}_{i=0}^n$.

Given an ensemble of identical quantum states ρ, on which individual measurements are performed, one obtains the probability distribution $\Pr(i|\rho) = \mathrm{tr}[M_i\rho]$ for the set of detectors described by the POVM elements M_i. Collecting all outputs, one can compute

$$\mathrm{tr}[W\rho] = \sum_{i=1}^{n} c_i \Pr(i|\rho). \tag{D.3}$$

If equation (D.3) yields a negative value, we unambiguously conclude that the given state ρ is entangled.

As it is mentioned above, entanglement witnesses can be factorized into local observables, that is, local measurements. A POVM element of local measurements can be written as

$$M_i = M_a^x \otimes M_b^y,$$

with indices $i = (x, y, a, b)$, where M_a^x denotes a POVM element having outcome a for measurement setting x. Suppose that witness W has a decomposition containing only local measurements, i.e.

$$W = \sum_{a,b,x,y} c_{a,b}^{x,y} M_a^x \otimes M_b^y.$$

Then, the detection scheme with local measurements is given by the relation

$$\mathrm{tr}[W\rho] = \sum_{a,b,x,y} c_{a,b}^{x,y} \Pr(a, b|x, y), \tag{D.4}$$

where $\Pr(a, b|x, y) = \mathrm{tr}[M_a^x \otimes M_b^y \rho]$ and the parameters $\{c_{a,b}^{x,y}\}$ can be found from the witness W.

We now introduce an equivalent scheme for detecting entangled states by modifying an entanglement witness as follows. Let $X \in \mathcal{B}(\mathcal{H} \otimes \mathcal{H})$ denote a non-negative, full-rank and unit-trace operator. Then, for a witness W, and an operator X, we define the following transformation

$$W_X(p) = (1 - p)W + p\,X, \tag{D.5}$$

with parameter $0 \leqslant p \leqslant 1$. Note that we have the relation, $W = W_X(p = 0)$. Since X is non-negative and of full-rank, it holds that for all separable states σ_{sep}

$$\mathrm{tr}[W_X(p)\sigma_{\mathrm{sep}}] \geqslant p\; m_s(X), \tag{D.6}$$

where $m_s(X) = \min_{\sigma_{\mathrm{sep}}} \mathrm{tr}[X\sigma_{\mathrm{sep}}]$. In the minimization of

$$m_s(X) = \min_{|a\rangle,|b\rangle} \mathrm{tr}[|a\rangle\langle a| \otimes |b\rangle\langle b|X], \tag{D.7}$$

it sufficed to consider product states since mixing does not decrease the norm of the above quantity.

Inequalities satisfied by separable states can therefore be constructed from equation (D.6) as follows. Assume that $W_X(p)$ has a separable decomposition

$$W_X(p) = \sum_{a,b,x,y} \tilde{c}_{a,b}^{x,y} M_a^x \otimes M_b^y, \tag{D.8}$$

for some fixed p, and let $P(a, b, |x, y) = \mathrm{tr}[M_a^x \otimes M_b^y \rho]$, for a given state ρ. Then it follows directly from equation (D.6) that the inequality

$$\sum_{x,y,a,b} \tilde{c}_{a,b}^{x,y} P(a, b|x, y) \geqslant p\; m_s(X), \tag{D.9}$$

is satisfied for all separable states. A violation of the inequality leads to the conclusion that the given quantum state ρ is entangled.

D.1.1. Lower bounds $L_{d^2,d}^{(\mathrm{S})}$ and $L_{d+1,d}^{(\mathrm{M})}$. We now derive the lower bounds $L_{d^2,d}^{(\mathrm{S})}$ and $L_{d+1,d}^{(\mathrm{M})}$ for sets of d^2 SIC vectors and $(d + 1)$ MUBs, i.e. quantum 2-designs. First, we consider equation (D.5) with the following operators

$$W = (id \otimes T)[|\Phi^+\rangle\langle\Phi^+|], \quad \text{and} \quad X_0 = \frac{1}{d^2}\mathbb{1}_d \otimes \mathbb{1}_d,$$

where $|\Phi^+\rangle = \sum_{i=1}^d |ii\rangle/\sqrt{d}$, is the maximally entangled state in $\mathbb{C}^d \otimes \mathbb{C}^d$. Note that $W = |\Phi^+\rangle\langle\Phi^+|^\Gamma$, where Γ denotes the partial transpose, corresponds to the permutation operator Π, i.e. $W = d^{-1}(\Pi_{\mathrm{sym}} - \Pi_{\mathrm{asym}})$ where Π_{sym} and Π_{asym} denote the projectors onto the symmetric and anti-symmetric subspaces. We also fix $p^* = d(d + 1)^{-1}$ so that $W_{X_0}(p^*)$ is non-negative. This is called the structural physical approximation of the witness [1]. Finally, equation (D.5) can be expressed as,

$$W_{X_0}(p^*) = \frac{2}{d(d+1)}\Pi_{\text{sym}}. \tag{D.10}$$

Thus, it follows that the lower bound for separable states in equation (D.6) is given by

$$\text{tr}[W_{X_0}(p^*)\sigma_{\text{sep}}] \geqslant \min_{\sigma_{\text{sep}}} p^* m_s(X_0) = \frac{1}{d(d+1)}, \tag{D.11}$$

where we have used the simple observation that $m_s(X_0) = d^{-2}$. It is clear that the resulting witness in equation (D.10) corresponds to a quantum 2-design (see equation (A.1)), and can therefore be decomposed using a full set of $(d+1)$ MUBs or d^2 SIC vectors. Thus, we can derive an inequalities of the form given in equation (D.9) using MUBs and SICs.

First, if we consider a quantum 2-design formed from a collection of d^2 SIC vectors, then equation (D.10) can be decomposed as,

$$\frac{2}{d(d+1)}\Pi_{\text{sym}} = \frac{1}{d^2}\sum_{j=1}^{d^2} |s_j\rangle\langle s_j| \otimes |s_j\rangle\langle s_j|.$$

Since the left-hand-side of equation (D.11) can be decomposed in terms of a SIC-POVM, the inequality can be rewritten as,

$$I^{(\text{S})}_{d^2,d} = \sum_{j=1}^{d^2} \Pr(j, j|S_{d^2}, S_{d^2}) \geqslant \frac{d}{d+1} = L^{(\text{S})}_{d^2,d}.$$

Thus, we have derived the lower bound $L^{(\text{S})}_{d^2,d} = d(d+1)^{-1}$.

Next, let us consider the case when the quantum 2-design in equation (D.10) is decomposed using a set of $(d+1)$ MUBs, i.e.

$$\frac{2}{d(d+1)}\Pi_{\text{sym}} = \frac{1}{d(d+1)}\sum_{k=1}^{d+1}\sum_{i=1}^{d} |b_i^k\rangle\langle b_i^k| \otimes |b_i^k\rangle\langle b_i^k|.$$

The left-hand-side of equation (D.11) is then written in terms of a set of MUBs, so that

$$I^{(\text{M})}_{d+1,d} = \sum_{k=1}^{d+1}\sum_{i=1}^{d} \Pr(i, i|\mathcal{B}_k, \mathcal{B}_k) \geqslant 1 = L^{(\text{M})}_{d+1,d}.$$

Thus, we have shown that $L^{(\text{M})}_{d+1,d} = 1$.

D.1.2. Upper bounds $U^{(\text{S})}_{d^2,d}$ and $U^{(\text{M})}_{d+1,d}$. The upper bounds $U^{(\text{M})}_{d+1,d}$ and $U^{(\text{S})}_{d^2,d}$ for a complete set of MUBs and a SIC-POVM, respectively, can be derived via applications of the geometric mean [14, 17]. For the upper bound in equation (B.18), a separable state can be decomposed into a convex combination of product states, and due to the convexity it suffices to consider product states in the optimization. Therefore, we have

$$\begin{aligned} I^{(\text{S})}_{d^2,d}(\sigma_{\text{sep}}) &\leqslant \max_{|e\rangle,|f\rangle} \sum_{j=1}^{d^2} \text{tr}[|s_j\rangle\langle s_j|^{\otimes 2} |e\rangle\langle e| \otimes |f\rangle\langle f|] \\ &\leqslant \max_{|e\rangle,|f\rangle} \sum_{j=1}^{d^2} \frac{1}{2}(|\langle s_j|e\rangle|^4 + |\langle s_j|f\rangle|^4|) \qquad \text{(D.12)} \\ &= \max_{|e\rangle} \sum_{j=1}^{d^2} |\langle s_j|e\rangle|^4, \qquad \text{(D.13)} \end{aligned}$$

where the geometric mean is applied in the second inequality, $\frac{1}{n}\sum_{j=1}^{n} x_j \geqslant (\Pi_{j=1}^{n} x_j)^{1/n}$. Given that $\sum_{j=1}^{d^2}\langle s_j|\rho|s_j\rangle^2/d^2 = (1 + \text{tr}(\rho^2))/(d(d+1))$, as shown in [49], the upper bound takes the value $U^{(\text{S})}_{d^2,d} = 2d(d+1)^{-1}$. A similar approach yields the inequality

$$I^{(\text{M})}_{d+1,d}(\sigma_{\text{sep}}) \leqslant \max_{|e\rangle} \sum_{k=1}^{d+1}\sum_{i=1}^{d} |\langle b_i^k|e\rangle|^4, \tag{D.14}$$

for a complete set of MUBs. Using $\sum_{k=1}^{d+1}\sum_{i=1}^{d}\langle b_i^k|\rho|b_i^k\rangle^2 = 1 + \text{tr}(\rho^2)$, as shown in [50], we find $U^{(\text{M})}_{d+1,d} = 2$. Thus, to summarize, when sets of MUBs and SIC vectors form a quantum 2-design, we have

$$1 \leqslant I^{(\text{M})}_{d+1,d}(\sigma_{\text{sep}}) \leqslant 2, \tag{D.15}$$

$$\frac{d}{d+1} \leqslant I^{(\text{S})}_{d^2,d}(\sigma_{\text{sep}}) \leqslant \frac{2d}{d+1}. \tag{D.16}$$

We note that these bounds have been obtained independently in [14, 15, 17].

ORCID iDs

Joonwoo Bae https://orcid.org/0000-0002-2345-1619
Beatrix C Hiesmayr https://orcid.org/0000-0001-9062-6039

References

[1] Horodecki P and Ekert A 2002 *Phys. Rev. Lett.* **89** 127902
[2] Shultz F 2016 *J. Math. Phys.* **57** 015218
Bae J 2017 *Rep. Prog. Phys.* **80** 10
[3] Terhal B M 2000 *Phys. Lett.* A **271** 319
[4] Gühne O and Toth G 2009 *Phys. Rep.* **474** 1
Chrúsciński D and Sarbicki G 2014 *J. Phys. A: Math. Theor.* **47** 483001
[5] Buscemi F 2012 *Phys. Rev. Lett.* **108** 200401
[6] Branciard C, Rosset D, Liang Y-C and Gisin N 2013 *Phys. Rev. Lett.* **110** 060405
[7] Cavalcanti E G, Hall M J W and Wiseman H M 2013 *Phys. Rev.* A **87** 032306
[8] Liang Y-C, Vertesi T and Brunner N 2011 *Phys. Rev.* A **83** 022108
[9] Horodecki M, Horodecki P and Horodecki R 1996 *Phys. Lett.* A **223** 1
[10] Terhal B M and Vollbrecht K G 2000 *Phys. Rev. Lett.* **85** 2625
Navascués M, Owari M and Plenio M 2009 *Phys. Rev. Lett.* **103** 160404
Brandão F G S L and Christandl M 2012 *Phys. Rev. Lett.* **109** 160502
[11] Lu D *et al* 2016 *Phys. Rev. Lett.* **116** 230501
[12] Schwinger J 1960 *Proc. Natl Acad. Sci. USA* **46** 570
[13] Renes J M, Blume-Kohout R, Scott A J and Caves C M 2004 *J. Math. Phys.* **45** 2171
[14] Spengler C, Huber M, Brierley S, Adaktylos T and Hiesmayr B C 2012 *Phys. Rev.* A **86** 022311
[15] Kalev A and Bae J 2013 *Phys. Rev.* A **87** 062314
[16] Chen B, Ma T and Fei S-M 2014 *Phys. Rev.* A **89** 064302
[17] Chen B, Li T and Fei S-M 2015 *Quantum Inf. Process.* **14** 2281
[18] Graydon M A and Appleby D M 2016 *J. Phys. A: Math. Theor.* **49** 085301
[19] Hiesmayr B C and Löffler W 2013 *New J. Phys.* **15** 083036
Hiesmayr B C and Löffler W 2014 *Phys. Scr.* **2014** 014017
[20] Horodecki M, Horodecki P and Horodecki R 1998 *Phys. Rev. Lett.* **80** 5239
[21] Wootters W K and Fields B D 1989 *Ann. Phys.* **191** 363
[22] Scott A J 2006 *J. Phys. A: Math. Gen.* **39** 13507
[23] Gühne O, Hyllus P, Bruss D, Ekert A, Lewenstein M, Macchiavello C and Sanpera A 2003 *J. Mod. Opt.* **50** 1079
[24] Paulsen V 2003 *Completely Bounded Maps and Operator Algebras* vol 78 (Cambridge: Cambridge University Press)
[25] The 13th open quantum problem, in https://oqp.iqoqi.univie.ac.at/open-quantum-problems
The 23rd open quantum problem, in https://oqp.iqoqi.univie.ac.at/open-quantum-problems
[26] Ivanovic I D 1981 *J. Phys. A: Math. Gen.* **14** 3241
[27] Bandyopadhyay S, Boykin P O, Roychowdhury V and Vatan F 2002 *Algorithmica* **34** 512
Klappenecker A and Rötteler M 2004 Constructions of mutually unbiased bases *Finite Fields and Applications. Fq 2003* (*Lecture Notes in Computer Science* vol 2948) ed G L Mullen, A Poli and H Stichtenoth (Berlin: Springer) pp 137–44
Durt T 2005 *J. Phys. A: Math. Gen.* **38** 5267
[28] Spengler C and Kraus B 2013 *Phys. Rev.* A **88** 052323
[29] Durt T, Englert B-G, Bengtsson I and Życzkowski K 2010 *Int. J. Quantum. Inf.* **8** 535
[30] Grassl M 2004 *Proc. ERATO Conf. on Quantum Information Science 2004 (EQIS 2004)* arXiv:quant-ph/0406175
Brierley S and Weigert S 2008 *Phys. Rev.* A **78** 042312
Brierley S and Weigert S 2010 *J. Phys.: Conf. Ser.* **254** 012008
[31] Raynal P, Lu X and Englert B-G 2011 *Phys. Rev.* A **83** 062303
McNulty D and Weigert S 2012 *Int. J. Quantum Inf.* **10** 1250056
[32] Scott A J 2017 arXiv:1703.03993
[33] Bian Z, Li J, Qin H, Zhan X, Zhang R, Sanders B C and Xue P 2015 *Phys. Rev. Lett.* **114** 203602
[34] Roy A and Scott A J 2007 *J. Math. Phys.* **48** 072110
[35] Chruściński D, Sarbicki G and Wudarski F 2018 *Phys. Rev.* A **97** 032318
[36] Gühne O and Lütkenhaus N 2006 *Phys. Rev. Lett.* **96** 170502
[37] Kalev A and Gour G 2014 *New J. Phys.* **16** 053038
Kalev A and Gour G 2014 *J. Phys. A: Math. Theor.* **47** 335302
[38] Zauner G 2011 *Int. J. Quantum Inf.* **9** 445
[39] Fuchs C A, Hoang M C and Stacey B C 2017 *Axioms* **6** 21
[40] Kopp G S 2018 arXiv:1807.05877
[41] Grassl M, McNulty D, Mišta L Jr and Paterek T 2017 *Phys. Rev.* A **95** 012118
[42] Haagerup U 1997 *Operator Algebras and Quantum Field Theory* (Somerville, MA: International Press) pp 296–322
[43] Brierley S, Weigert S and Bengtsson I 2010 *Quantum Inf. Comput.* **10** 803
[44] Stacey B C 2017 *Found. Phys.* **47** 1060
[45] Veitch V, Mousavian S H, Gottesman D and Emerson J 2014 *New J. Phys.* **16** 013009
[46] Stacey B C 2016 *Mathematics* **4** 36
[47] Bengtsson I, Blanchfield K and Cabello A 2012 *Phys. Lett.* A **376** 374
Dang H B, Blanchfield K, Bengtsson I and Appleby D M 2013 *Quantum Inf. Process.* **12** 3449
[48] Tabia G N M and Appleby D M 2013 *Phys. Rev.* A **88** 012131
[49] Rastegin A E 2014 *Phys. Scr.* **89** 085101
[50] Larsen U 1990 *J. Phys. A: Math. Gen.* **23** 1041